FIG. 1

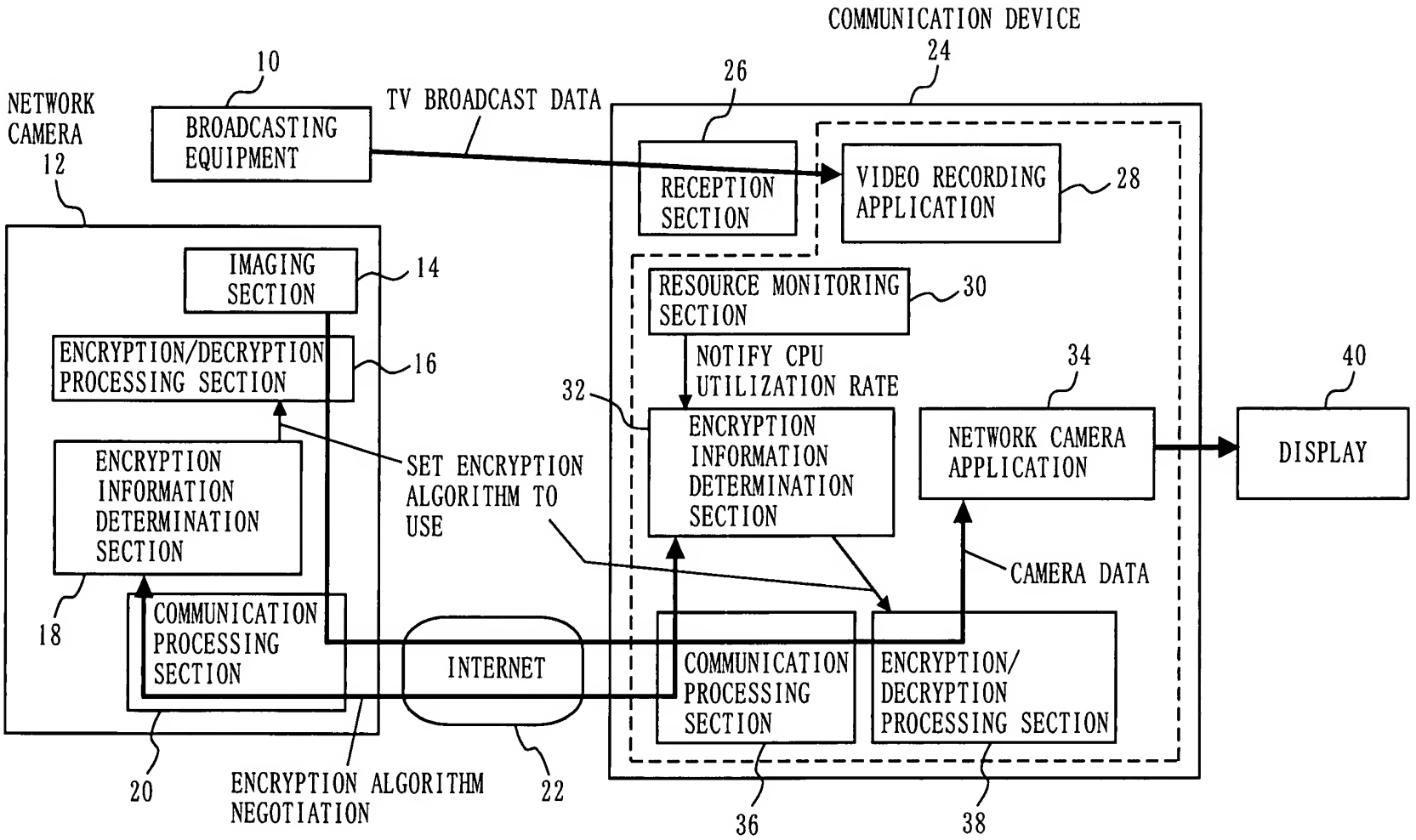
COMMUNICATION DEVICE
24
10
26
NETWORK CAMERA
12
BROADCASTING EQUIPMENT
TV BROADCAST DATA
RECEPTION SECTION
VIDEO RECORDING APPLICATION
28
IMAGING SECTION
14
RESOURCE MONITORING SECTION
30
ENCRYPTION/DECRYPTION PROCESSING SECTION
16
NOTIFY CPU UTILIZATION RATE
34
40
32
ENCRYPTION INFORMATION DETERMINATION SECTION
NETWORK CAMERA APPLICATION
DISPLAY
SET ENCRYPTION ALGORITHM TO USE
ENCRYPTION INFORMATION DETERMINATION SECTION
CAMERA DATA
18
COMMUNICATION PROCESSING SECTION
INTERNET
COMMUNICATION PROCESSING SECTION
ENCRYPTION/ DECRYPTION PROCESSING SECTION
20
ENCRYPTION ALGORITHM NEGOTIATION
22
36
38

FIG. 2

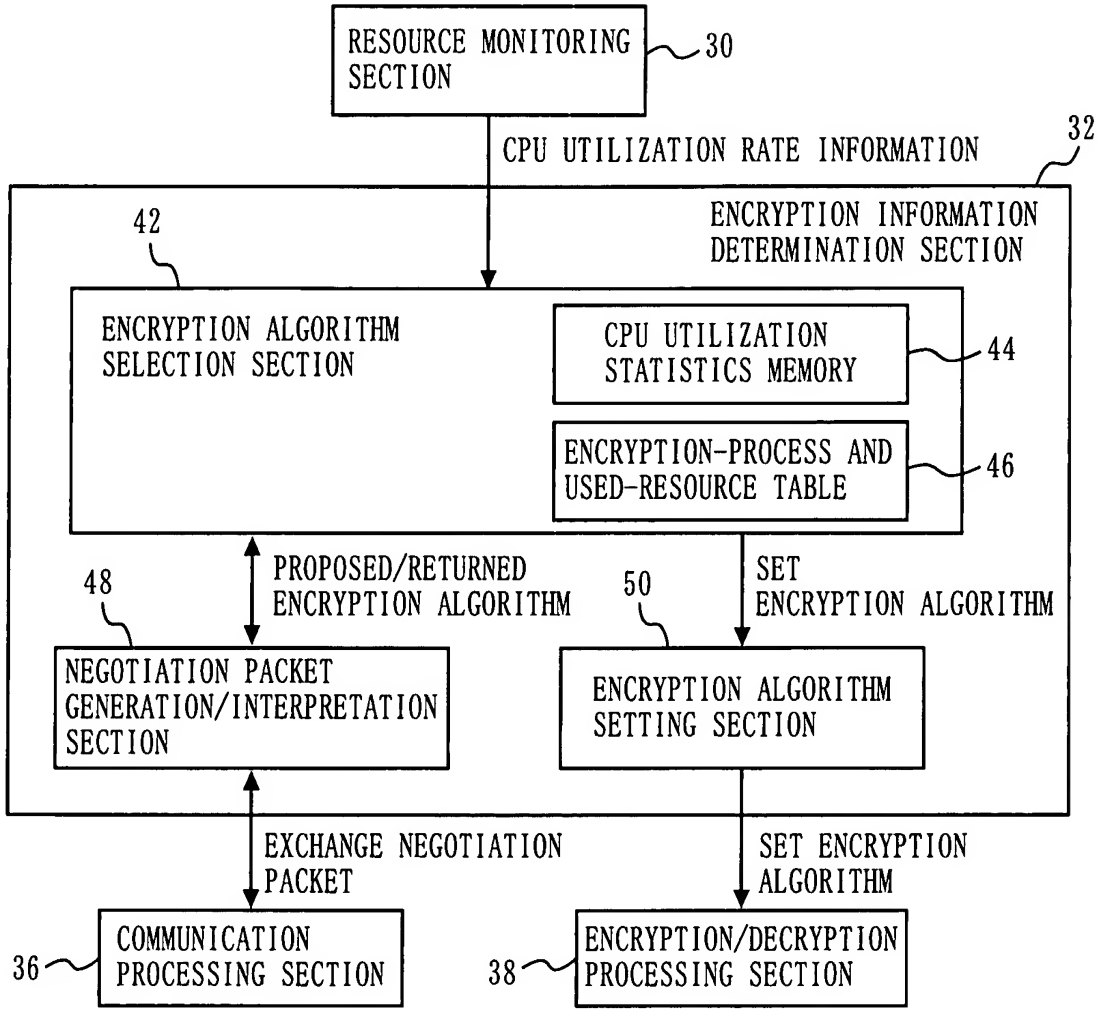
RESOURCE MONITORING SECTION
30
CPU UTILIZATION RATE INFORMATION
32
ENCRYPTION INFORMATION DETERMINATION SECTION
42
ENCRYPTION ALGORITHM SELECTION SECTION
CPU UTILIZATION STATISTICS MEMORY
44
ENCRYPTION-PROCESS AND USED-RESOURCE TABLE
46
PROPOSED/RETURNED ENCRYPTION ALGORITHM
48
50
SET ENCRYPTION ALGORITHM
NEGOTIATION PACKET GENERATION/INTERPRETATION SECTION
ENCRYPTION ALGORITHM SETTING SECTION
EXCHANGE NEGOTIATION PACKET
SET ENCRYPTION ALGORITHM
36
COMMUNICATION PROCESSING SECTION
38
ENCRYPTION/DECRYPTION PROCESSING SECTION

FIG. 3

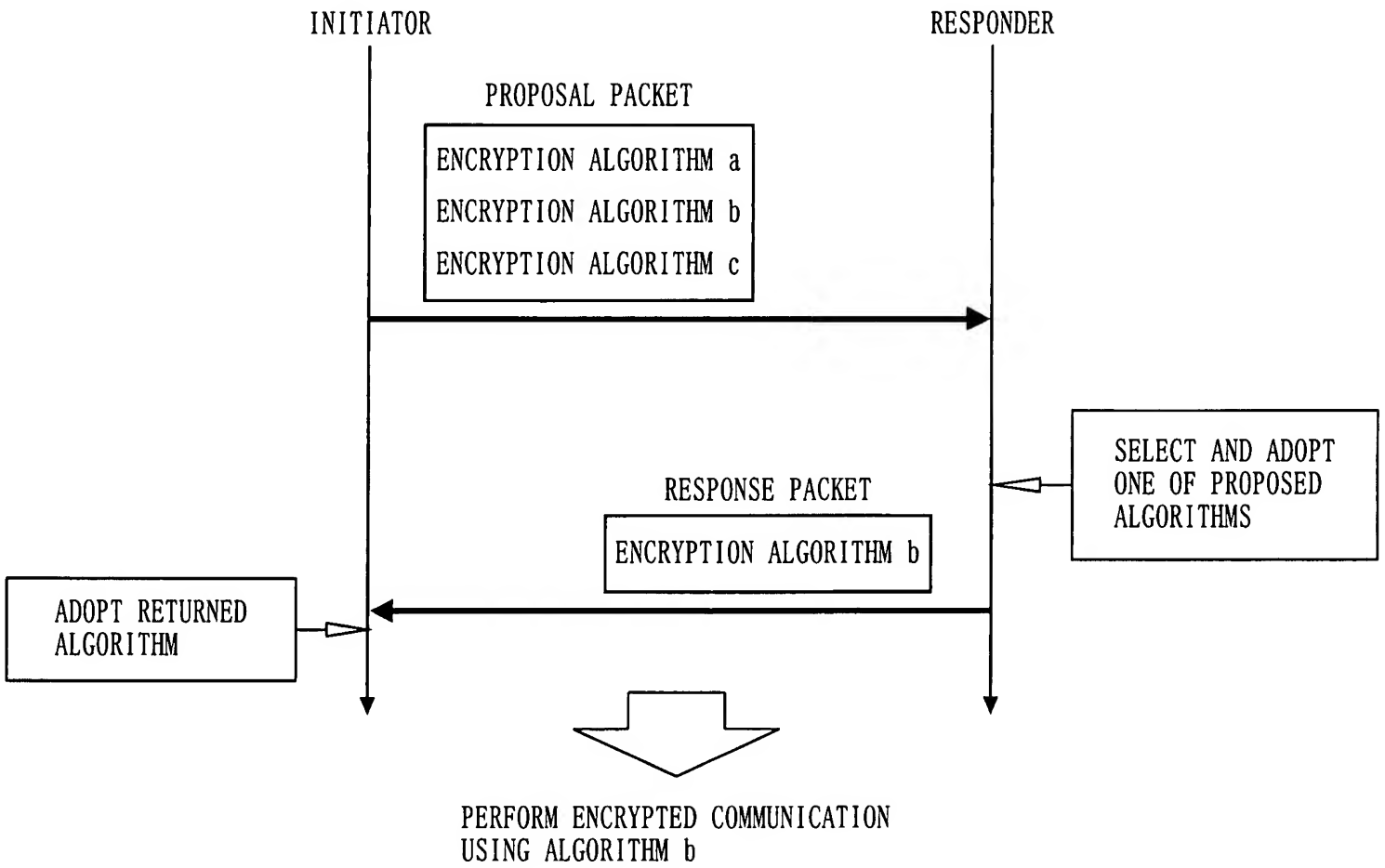
INITIATOR
RESPONDER
PROPOSAL PACKET
ENCRYPTION ALGORITHM a
ENCRYPTION ALGORITHM b
ENCRYPTION ALGORITHM c
SELECT AND ADOPT ONE OF PROPOSED ALGORITHMS
RESPONSE PACKET
ENCRYPTION ALGORITHM b
ADOPT RETURNED ALGORITHM
PERFORM ENCRYPTED COMMUNICATION USING ALGORITHM b

FIG. 4

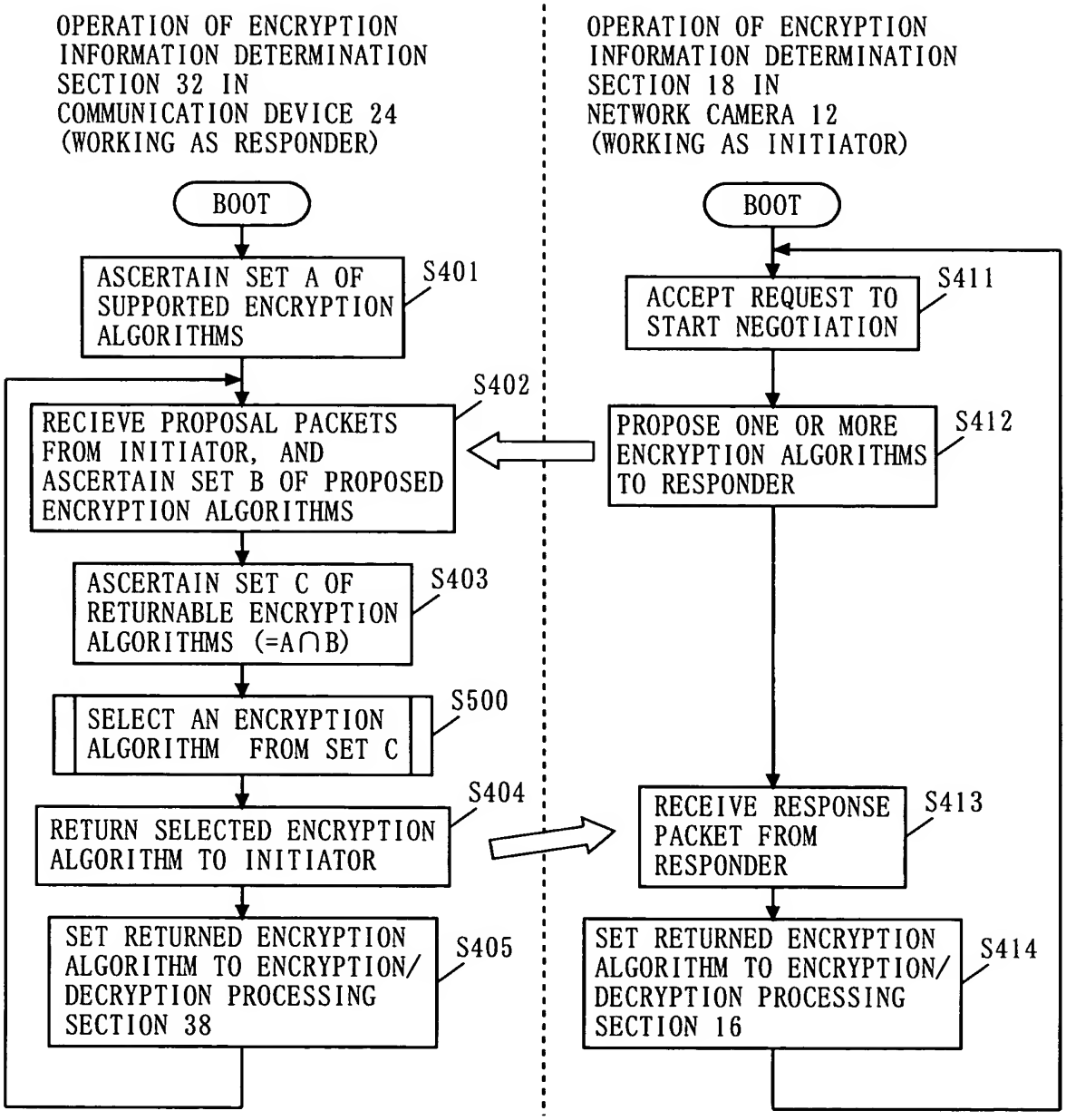
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 IN COMMUNICATION DEVICE 24 (WORKING AS RESPONDER)
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 IN NETWORK CAMERA 12 (WORKING AS INITIATOR)
BOOT
BOOT
ASCERTAIN SET A OF SUPPORTED ENCRYPTION ALGORITHMS
S401
ACCEPT REQUEST TO START NEGOTIATION
S411
S402
RECIEVE PROPOSAL PACKETS FROM INITIATOR, AND ASCERTAIN SET B OF PROPOSED ENCRYPTION ALGORITHMS
PROPOSE ONE OR MORE ENCRYPTION ALGORITHMS TO RESPONDER
S412
ASCERTAIN SET C OF RETURNABLE ENCRYPTION ALGORITHMS (=A∩B)
S403
SELECT AN ENCRYPTION ALGORITHM FROM SET C
S500
S404
RETURN SELECTED ENCRYPTION ALGORITHM TO INITIATOR
RECEIVE RESPONSE PACKET FROM RESPONDER
S413
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 38
S405
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 16
S414

FIG. 5

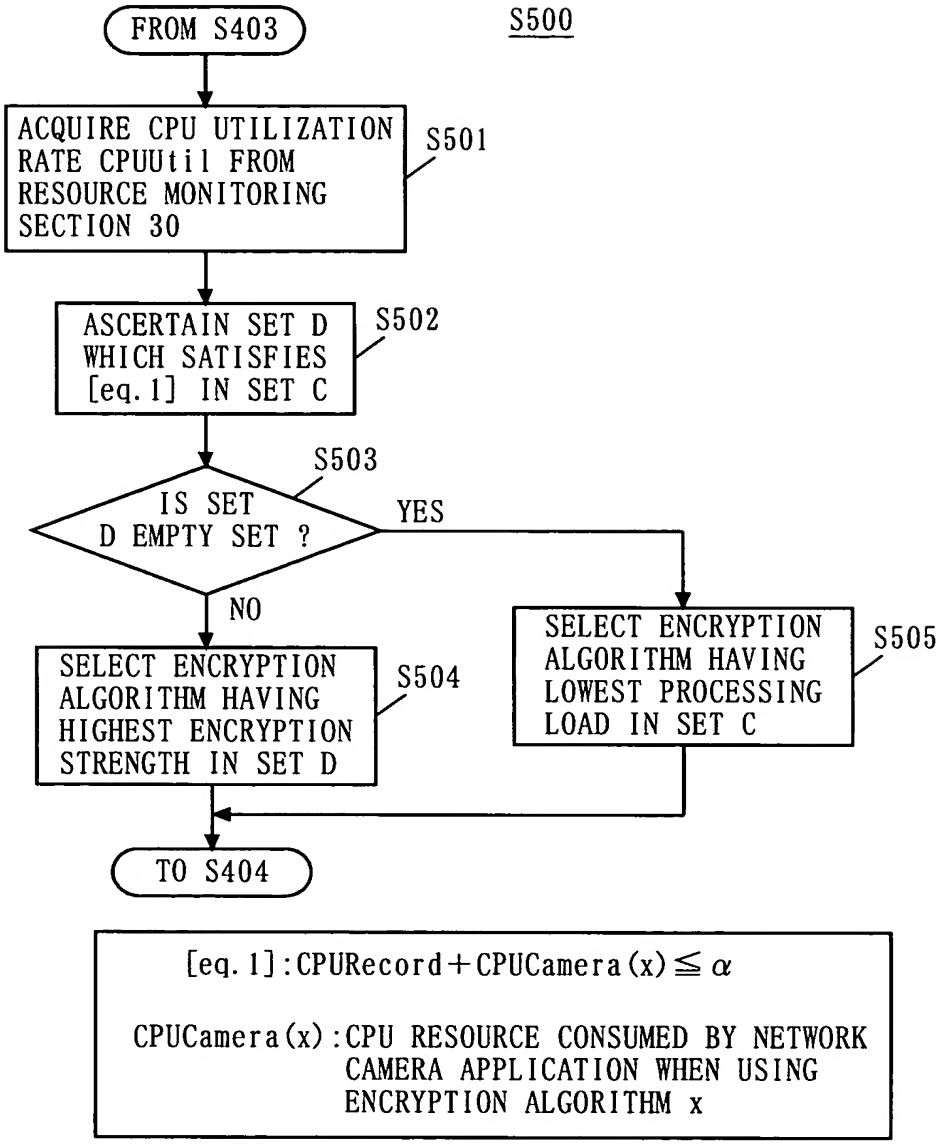
S500
FROM S403
ACQUIRE CPU UTILIZATION RATE CPUUtil FROM RESOURCE MONITORING SECTION 30
S501
ASCERTAIN SET D WHICH SATISFIES [eq.1] IN SET C
S502
S503
IS SET D EMPTY SET ?
YES
NO
SELECT ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH IN SET D
S504
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET C
S505
TO S404
[eq.1]:CPURecord+CPUCamera(x)≦α
CPUCamera(x):CPU RESOURCE CONSUMED BY NETWORK CAMERA APPLICATION WHEN USING ENCRYPTION ALGORITHM x

FIG. 6

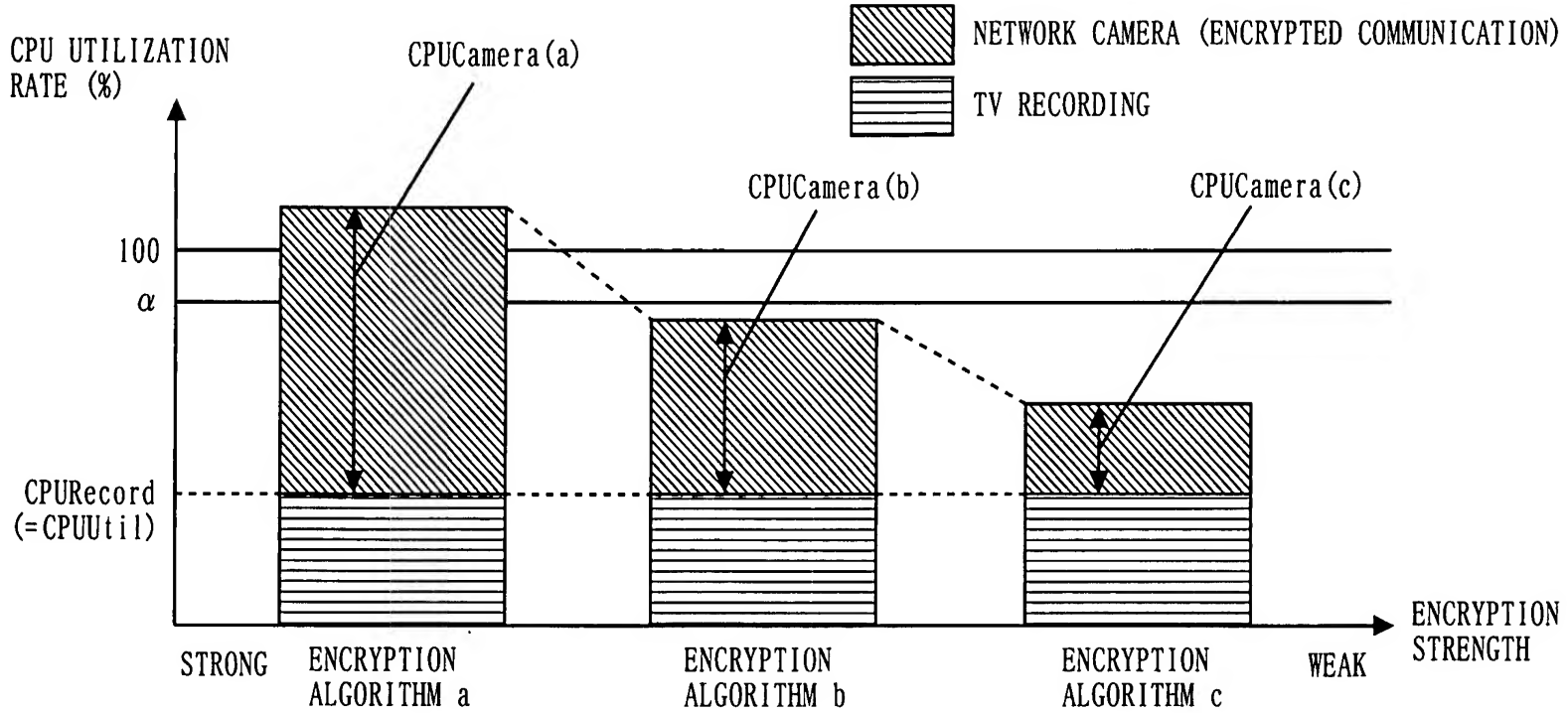
CPU UTILIZATION RATE (%)
CPUCamera(a)
NETWORK CAMERA (ENCRYPTED COMMUNICATION)
TV RECORDING
CPUCamera(b)
CPUCamera(c)
100
α
CPURecord (=CPUUtil)
STRONG
ENCRYPTION ALGORITHM a
ENCRYPTION ALGORITHM b
ENCRYPTION ALGORITHM c
WEAK
ENCRYPTION STRENGTH

FIG. 7

ENCRYPTION ALGORITHM	EncRate( )	ENCRYPTION STRENGTH
a	20	1
b	40	2
c	70	3
:	:	:

FIG. 8

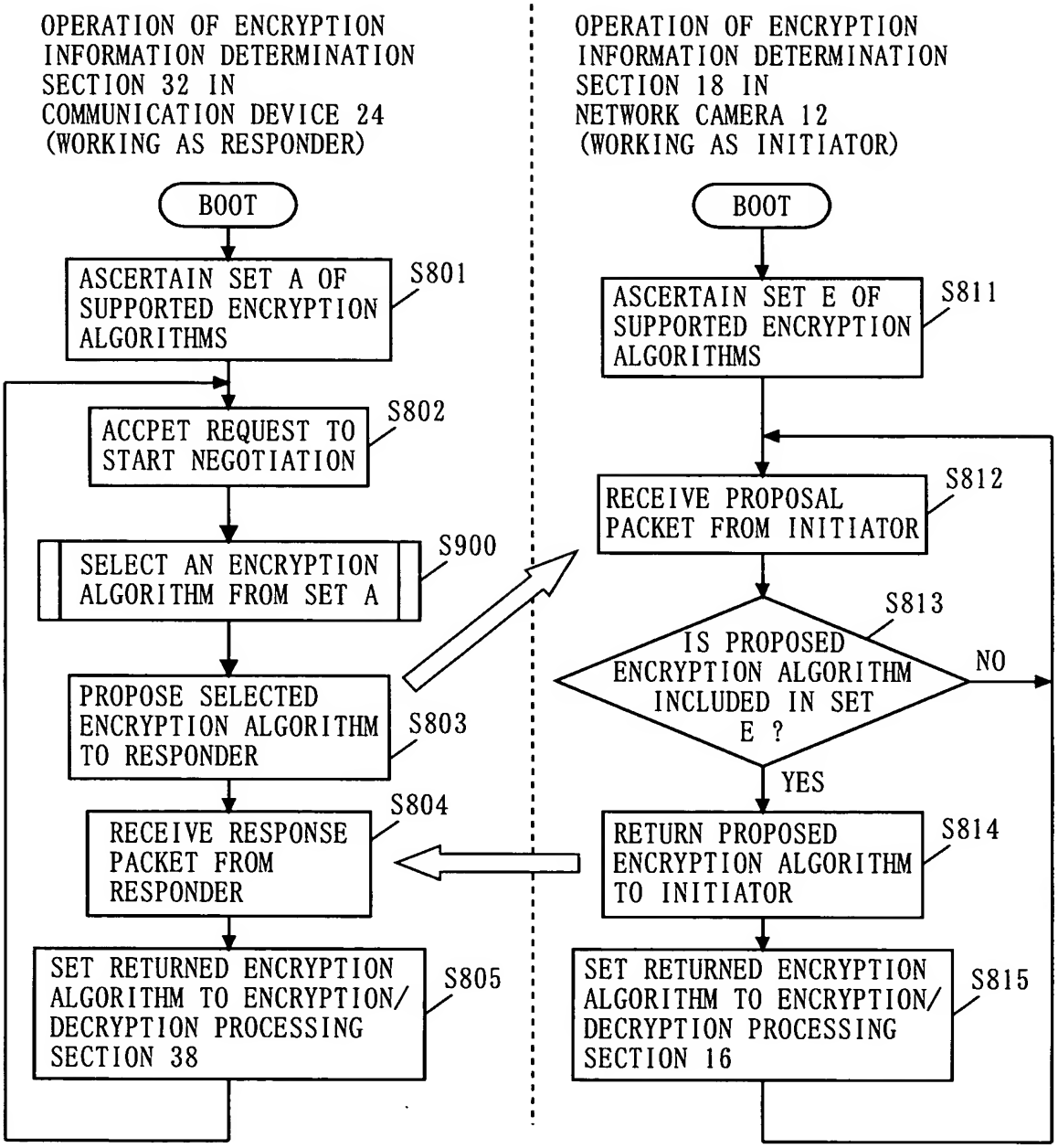
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 IN COMMUNICATION DEVICE 24 (WORKING AS RESPONDER)
BOOT
ASCERTAIN SET A OF SUPPORTED ENCRYPTION ALGORITHMS
S801
ACCPET REQUEST TO START NEGOTIATION
S802
SELECT AN ENCRYPTION ALGORITHM FROM SET A
S900
PROPOSE SELECTED ENCRYPTION ALGORITHM TO RESPONDER
S803
RECEIVE RESPONSE PACKET FROM RESPONDER
S804
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 38
S805
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 IN NETWORK CAMERA 12 (WORKING AS INITIATOR)
BOOT
ASCERTAIN SET E OF SUPPORTED ENCRYPTION ALGORITHMS
S811
RECEIVE PROPOSAL PACKET FROM INITIATOR
S812
IS PROPOSED ENCRYPTION ALGORITHM INCLUDED IN SET E ?
S813
NO
YES
RETURN PROPOSED ENCRYPTION ALGORITHM TO INITIATOR
S814
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 16
S815

FIG. 9

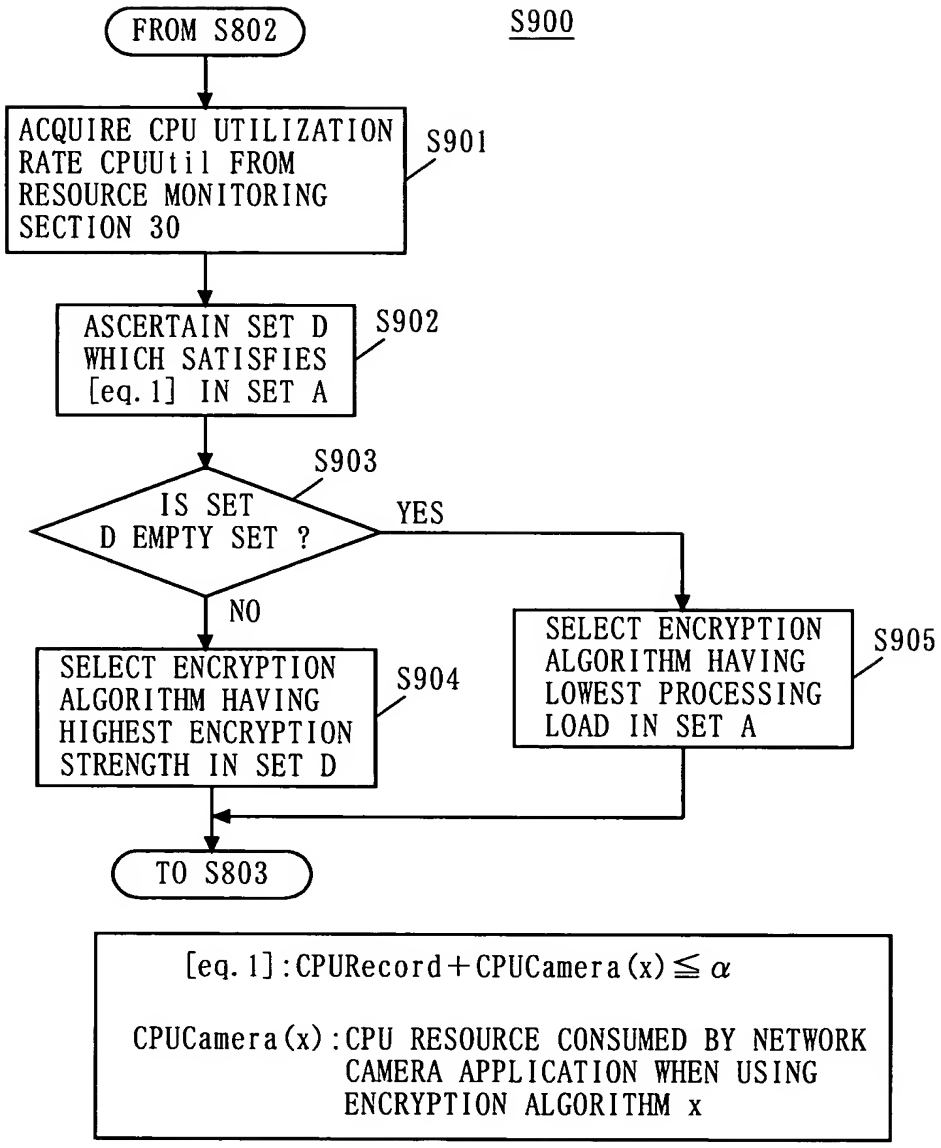
FROM S802
S900
ACQUIRE CPU UTILIZATION RATE CPUUtil FROM RESOURCE MONITORING SECTION 30
S901
ASCERTAIN SET D WHICH SATISFIES [eq. 1] IN SET A
S902
S903
IS SET D EMPTY SET ?
YES
NO
SELECT ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH IN SET D
S904
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET A
S905
TO S803
[eq. 1] : CPURecord + CPUCamera(x) ≦ α
CPUCamera(x) : CPU RESOURCE CONSUMED BY NETWORK CAMERA APPLICATION WHEN USING ENCRYPTION ALGORITHM x

FIG. 10

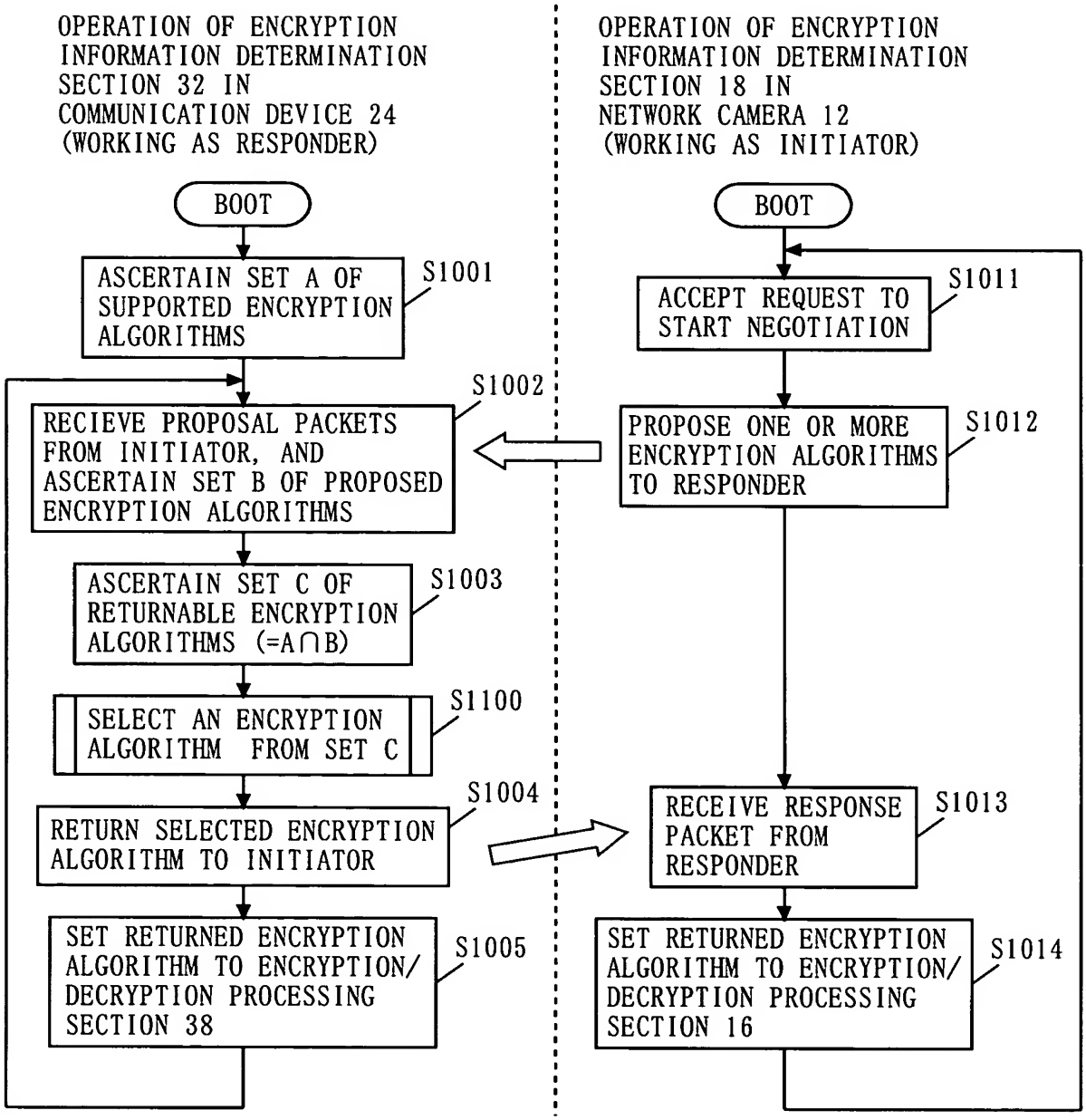
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 IN COMMUNICATION DEVICE 24 (WORKING AS RESPONDER)
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 IN NETWORK CAMERA 12 (WORKING AS INITIATOR)
BOOT
BOOT
ASCERTAIN SET A OF SUPPORTED ENCRYPTION ALGORITHMS
S1001
ACCEPT REQUEST TO START NEGOTIATION
S1011
S1002
RECIEVE PROPOSAL PACKETS FROM INITIATOR, AND ASCERTAIN SET B OF PROPOSED ENCRYPTION ALGORITHMS
PROPOSE ONE OR MORE ENCRYPTION ALGORITHMS TO RESPONDER
S1012
ASCERTAIN SET C OF RETURNABLE ENCRYPTION ALGORITHMS (=A∩B)
S1003
SELECT AN ENCRYPTION ALGORITHM FROM SET C
S1100
S1004
RETURN SELECTED ENCRYPTION ALGORITHM TO INITIATOR
RECEIVE RESPONSE PACKET FROM RESPONDER
S1013
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 38
S1005
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 16
S1014

FIG. 11

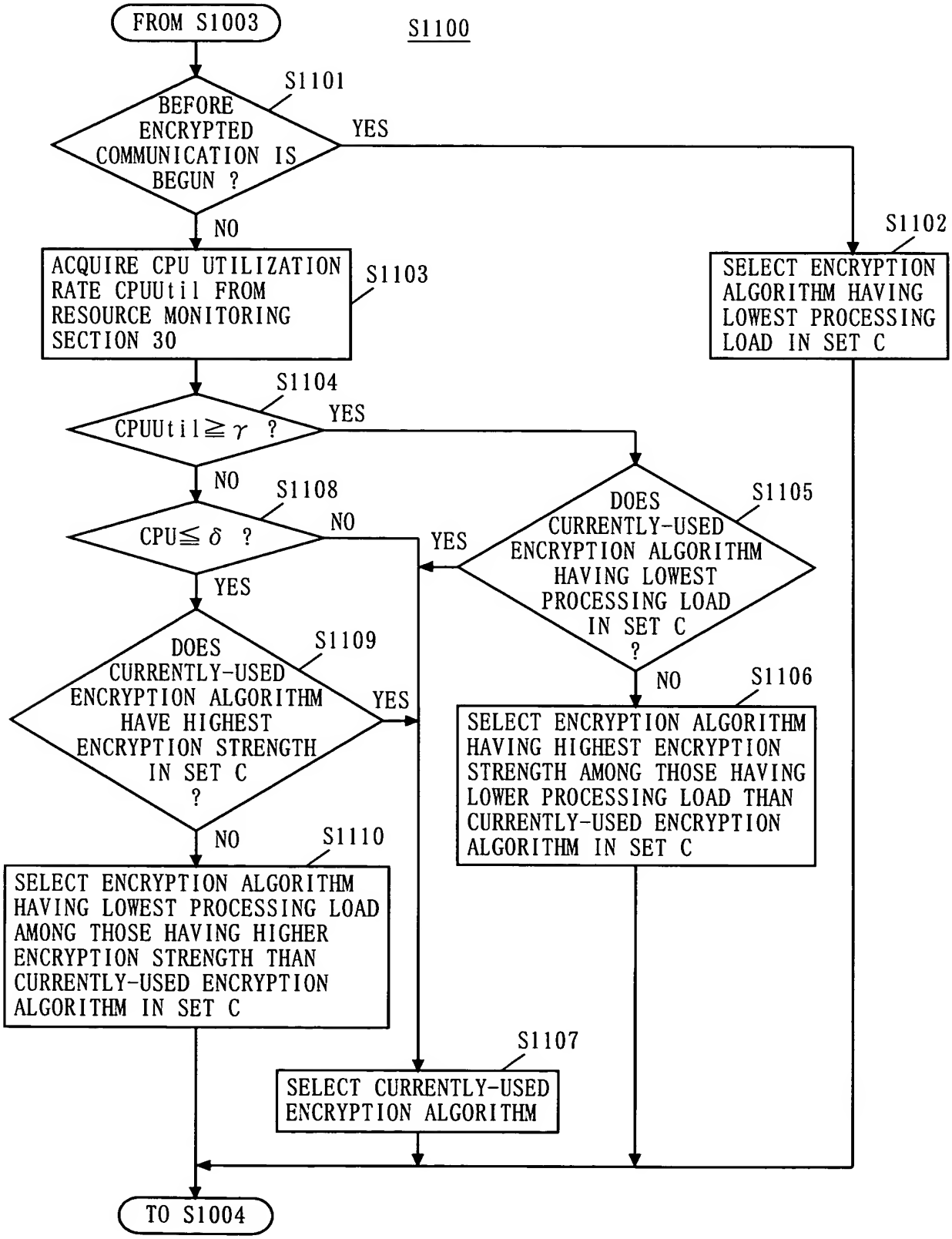
FROM S1003
S1100
S1101
BEFORE ENCRYPTED COMMUNICATION IS BEGUN ?
YES
NO
S1102
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET C
ACQUIRE CPU UTILIZATION RATE CPUUtil FROM RESOURCE MONITORING SECTION 30
S1103
S1104
CPUUtil≧γ ?
YES
NO
S1108
CPU≦δ ?
NO
YES
S1105
DOES CURRENTLY-USED ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET C ?
YES
NO
S1109
DOES CURRENTLY-USED ENCRYPTION ALGORITHM HAVE HIGHEST ENCRYPTION STRENGTH IN SET C ?
YES
NO
S1106
SELECT ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH AMONG THOSE HAVING LOWER PROCESSING LOAD THAN CURRENTLY-USED ENCRYPTION ALGORITHM IN SET C
S1110
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD AMONG THOSE HAVING HIGHER ENCRYPTION STRENGTH THAN CURRENTLY-USED ENCRYPTION ALGORITHM IN SET C
S1107
SELECT CURRENTLY-USED ENCRYPTION ALGORITHM
TO S1004

FIG. 12

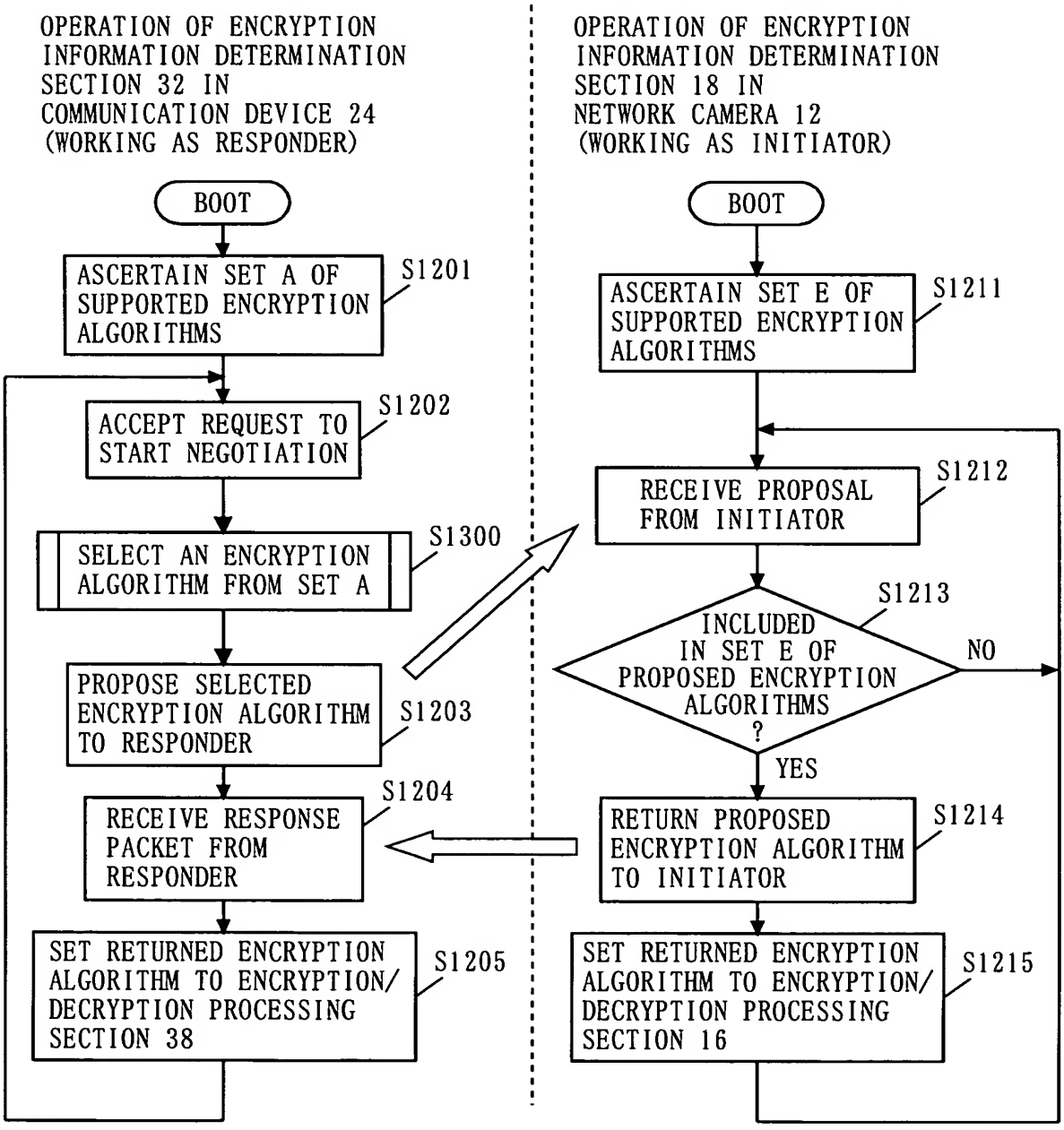
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 IN COMMUNICATION DEVICE 24 (WORKING AS RESPONDER)
BOOT
ASCERTAIN SET A OF SUPPORTED ENCRYPTION ALGORITHMS
S1201
ACCEPT REQUEST TO START NEGOTIATION
S1202
SELECT AN ENCRYPTION ALGORITHM FROM SET A
S1300
PROPOSE SELECTED ENCRYPTION ALGORITHM TO RESPONDER
S1203
RECEIVE RESPONSE PACKET FROM RESPONDER
S1204
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 38
S1205
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 IN NETWORK CAMERA 12 (WORKING AS INITIATOR)
BOOT
ASCERTAIN SET E OF SUPPORTED ENCRYPTION ALGORITHMS
S1211
RECEIVE PROPOSAL FROM INITIATOR
S1212
INCLUDED IN SET E OF PROPOSED ENCRYPTION ALGORITHMS ?
S1213
NO
YES
RETURN PROPOSED ENCRYPTION ALGORITHM TO INITIATOR
S1214
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 16
S1215

FIG. 13

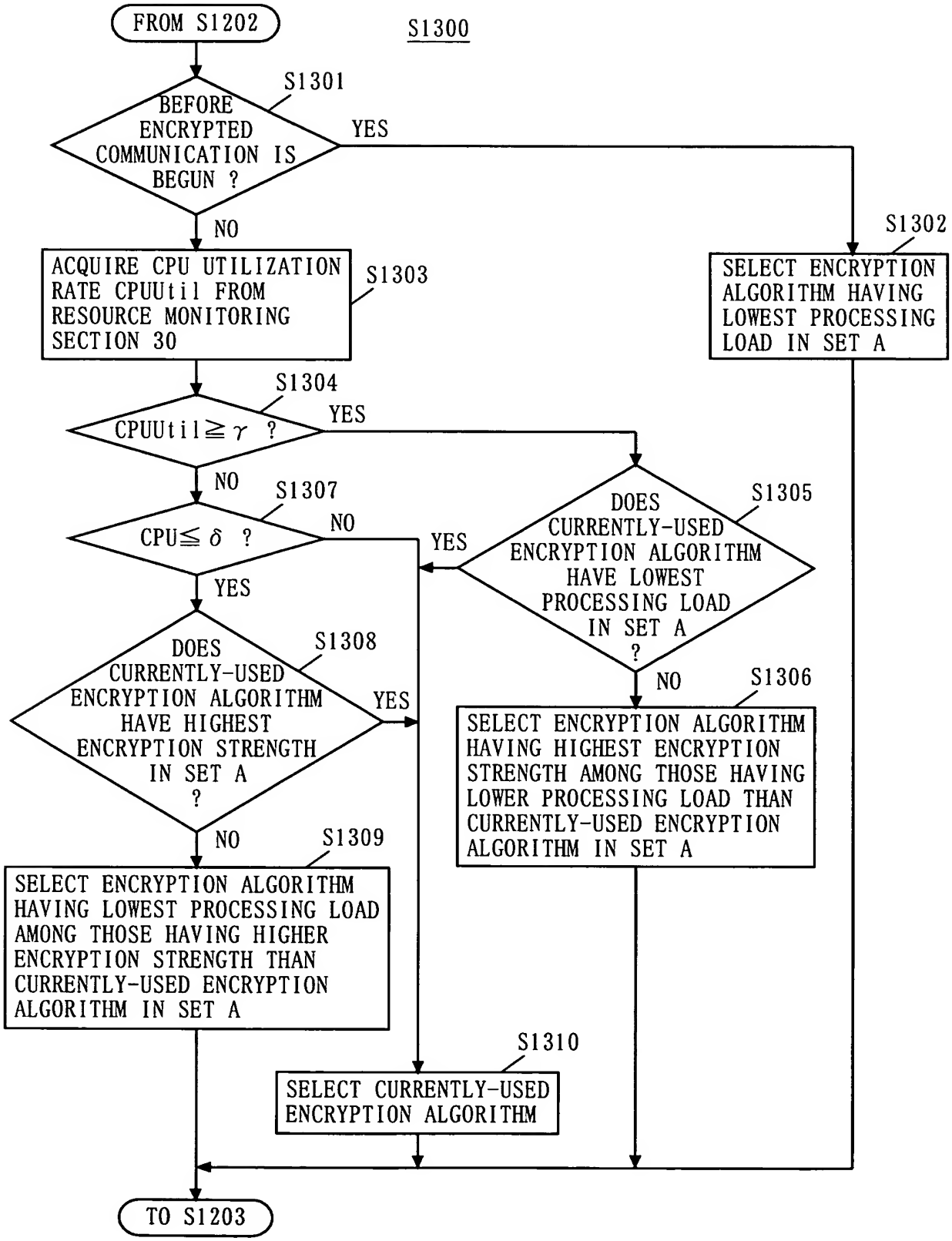
FROM S1202
S1300
S1301
BEFORE ENCRYPTED COMMUNICATION IS BEGUN ?
YES
NO
S1302
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET A
ACQUIRE CPU UTILIZATION RATE CPUUtil FROM RESOURCE MONITORING SECTION 30
S1303
S1304
CPUUtil≧γ ?
YES
NO
S1307
CPU≦δ ?
NO
YES
S1305
DOES CURRENTLY-USED ENCRYPTION ALGORITHM HAVE LOWEST PROCESSING LOAD IN SET A ?
YES
NO
S1308
DOES CURRENTLY-USED ENCRYPTION ALGORITHM HAVE HIGHEST ENCRYPTION STRENGTH IN SET A ?
YES
NO
S1306
SELECT ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH AMONG THOSE HAVING LOWER PROCESSING LOAD THAN CURRENTLY-USED ENCRYPTION ALGORITHM IN SET A
S1309
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD AMONG THOSE HAVING HIGHER ENCRYPTION STRENGTH THAN CURRENTLY-USED ENCRYPTION ALGORITHM IN SET A
S1310
SELECT CURRENTLY-USED ENCRYPTION ALGORITHM
TO S1203

FIG. 14

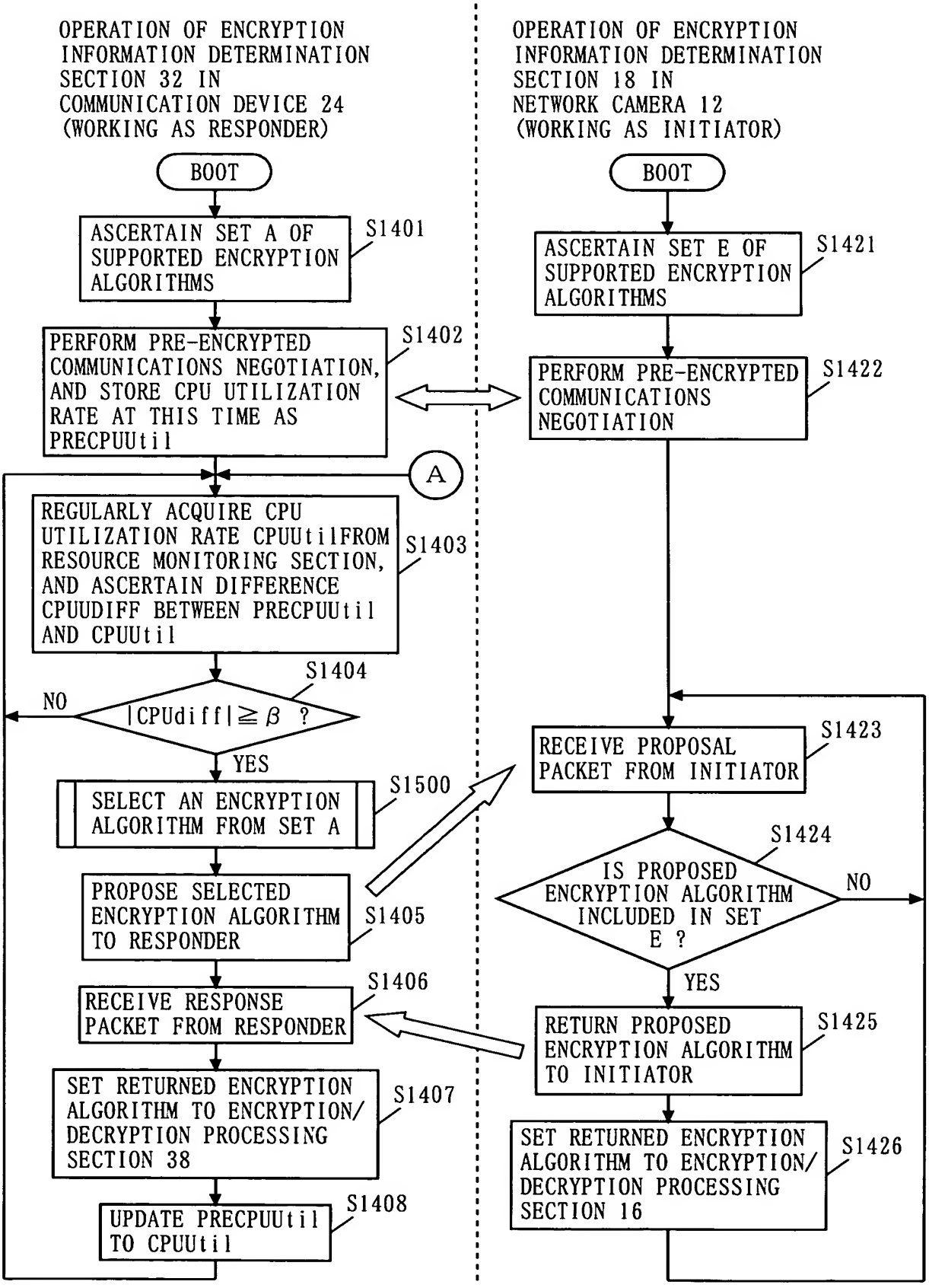
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 IN COMMUNICATION DEVICE 24 (WORKING AS RESPONDER)
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 IN NETWORK CAMERA 12 (WORKING AS INITIATOR)
BOOT
BOOT
ASCERTAIN SET A OF SUPPORTED ENCRYPTION ALGORITHMS
S1401
ASCERTAIN SET E OF SUPPORTED ENCRYPTION ALGORITHMS
S1421
PERFORM PRE-ENCRYPTED COMMUNICATIONS NEGOTIATION, AND STORE CPU UTILIZATION RATE AT THIS TIME AS PRECPUUtil
S1402
PERFORM PRE-ENCRYPTED COMMUNICATIONS NEGOTIATION
S1422
A
REGULARLY ACQUIRE CPU UTILIZATION RATE CPUUtilFROM RESOURCE MONITORING SECTION, AND ASCERTAIN DIFFERENCE CPUUDIFF BETWEEN PRECPUUtil AND CPUUtil
S1403
S1404
NO
|CPUdiff| ≧ β ?
YES
RECEIVE PROPOSAL PACKET FROM INITIATOR
S1423
SELECT AN ENCRYPTION ALGORITHM FROM SET A
S1500
S1424
IS PROPOSED ENCRYPTION ALGORITHM INCLUDED IN SET E ?
NO
PROPOSE SELECTED ENCRYPTION ALGORITHM TO RESPONDER
S1405
YES
S1406
RECEIVE RESPONSE PACKET FROM RESPONDER
RETURN PROPOSED ENCRYPTION ALGORITHM TO INITIATOR
S1425
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 38
S1407
SET RETURNED ENCRYPTION ALGORITHM TO ENCRYPTION/ DECRYPTION PROCESSING SECTION 16
S1426
UPDATE PRECPUUtil TO CPUUtil
S1408

FIG. 15

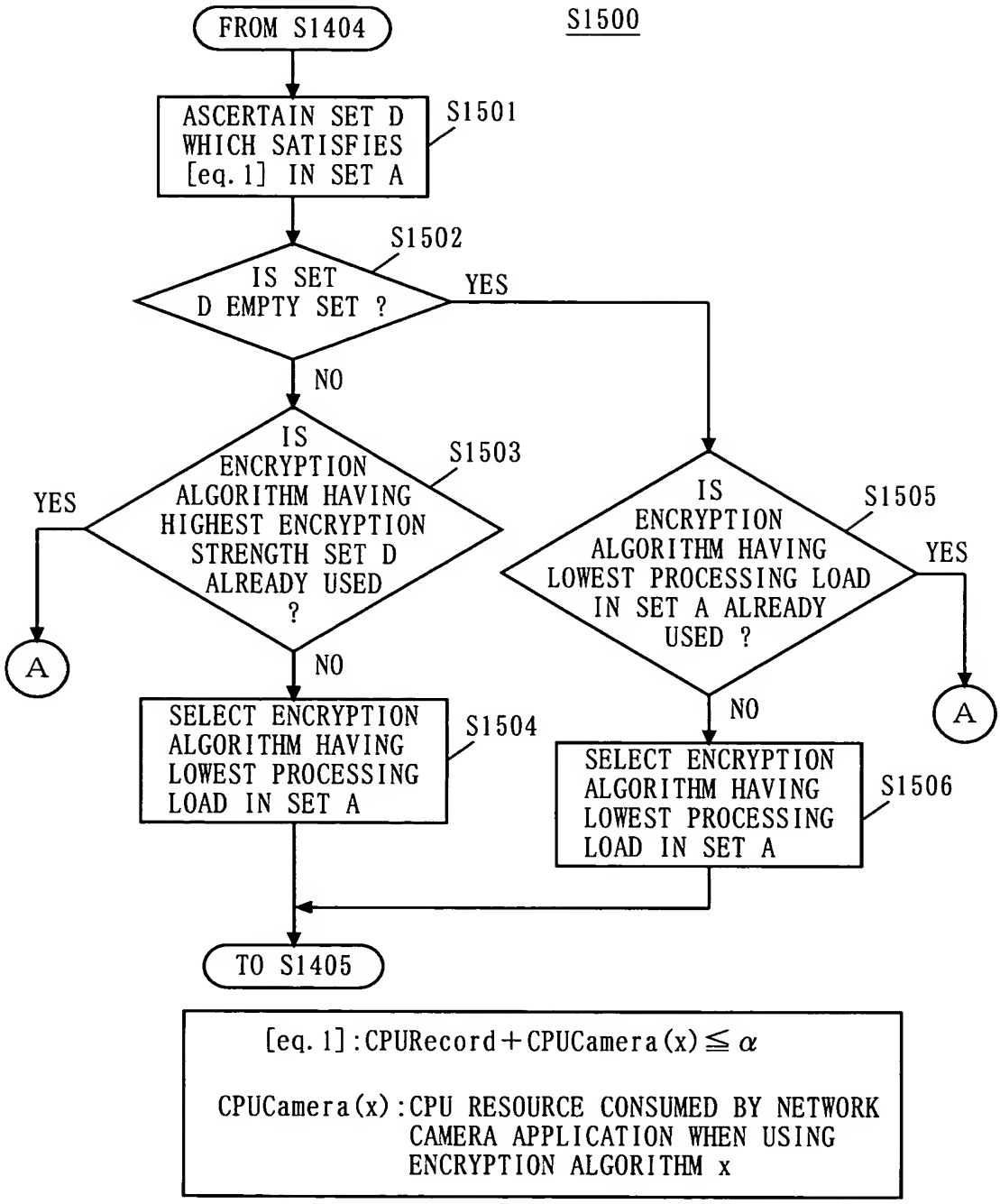
S1500
FROM S1404
ASCERTAIN SET D WHICH SATISFIES [eq. 1] IN SET A
S1501
S1502
IS SET D EMPTY SET ?
YES
NO
IS ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH SET D ALREADY USED ?
S1503
YES
A
NO
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET A
S1504
IS ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET A ALREADY USED ?
S1505
YES
A
NO
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET A
S1506
TO S1405
[eq. 1]:CPURecord+CPUCamera(x)≦α
CPUCamera(x):CPU RESOURCE CONSUMED BY NETWORK CAMERA APPLICATION WHEN USING ENCRYPTION ALGORITHM x

FIG. 16

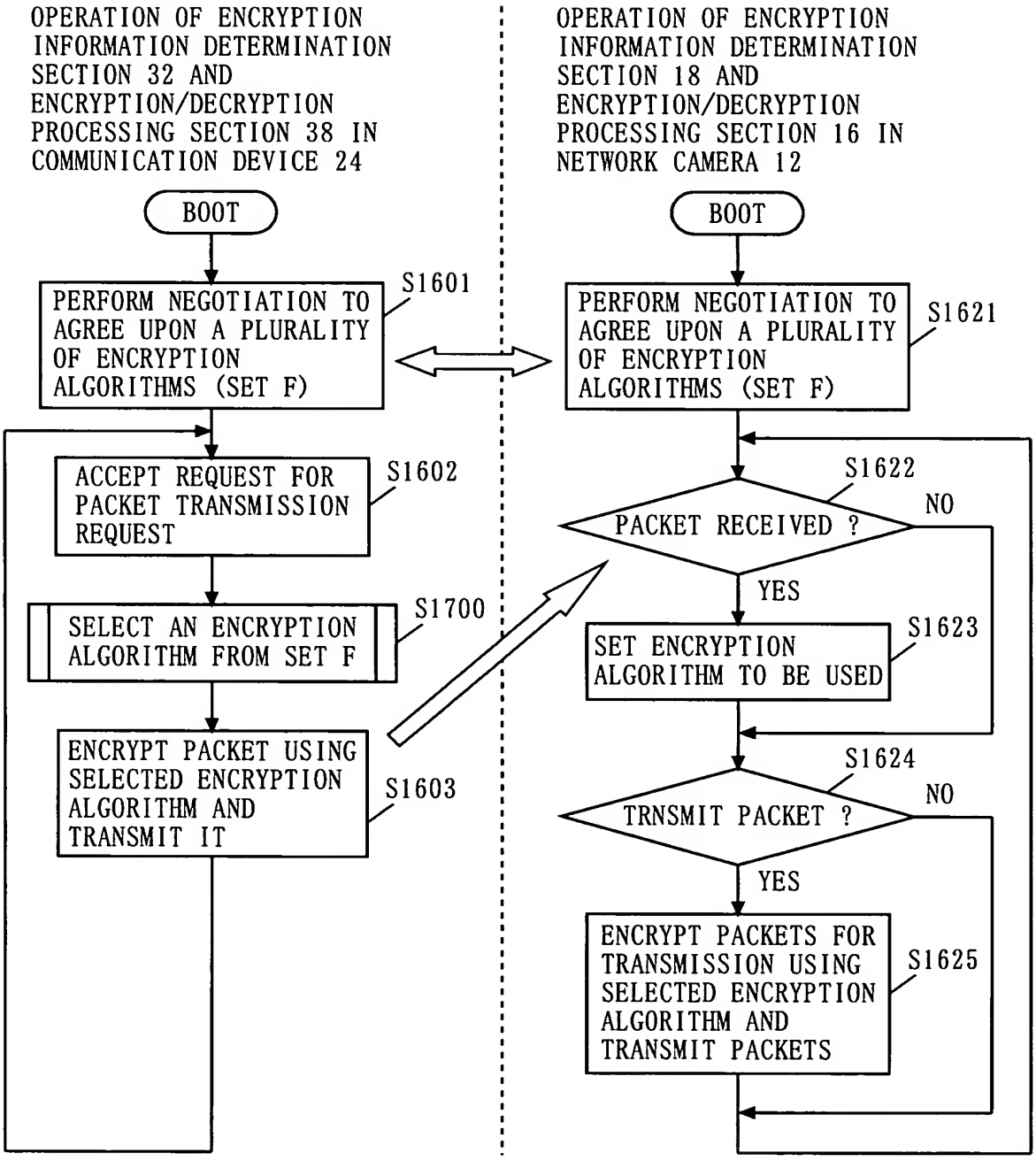
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 32 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 38 IN COMMUNICATION DEVICE 24
BOOT
PERFORM NEGOTIATION TO AGREE UPON A PLURALITY OF ENCRYPTION ALGORITHMS (SET F)
S1601
ACCEPT REQUEST FOR PACKET TRANSMISSION REQUEST
S1602
SELECT AN ENCRYPTION ALGORITHM FROM SET F
S1700
ENCRYPT PACKET USING SELECTED ENCRYPTION ALGORITHM AND TRANSMIT IT
S1603
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 18 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 16 IN NETWORK CAMERA 12
BOOT
PERFORM NEGOTIATION TO AGREE UPON A PLURALITY OF ENCRYPTION ALGORITHMS (SET F)
S1621
S1622
PACKET RECEIVED ?
NO
YES
SET ENCRYPTION ALGORITHM TO BE USED
S1623
S1624
TRNSMIT PACKET ?
NO
YES
ENCRYPT PACKETS FOR TRANSMISSION USING SELECTED ENCRYPTION ALGORITHM AND TRANSMIT PACKETS
S1625

FIG. 17

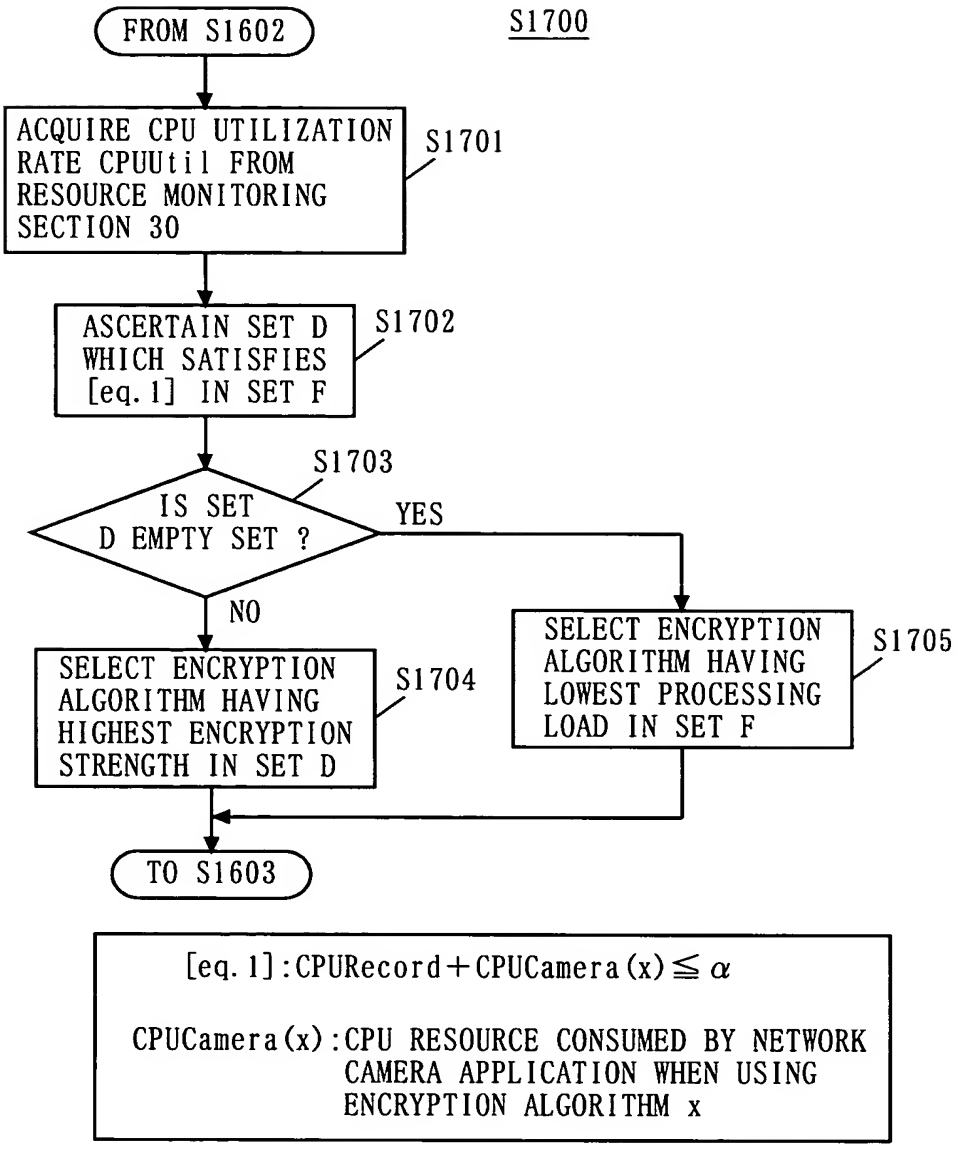
FROM S1602
S1700
ACQUIRE CPU UTILIZATION RATE CPUUtil FROM RESOURCE MONITORING SECTION 30
S1701
ASCERTAIN SET D WHICH SATISFIES [eq. 1] IN SET F
S1702
S1703
IS SET D EMPTY SET ?
YES
NO
SELECT ENCRYPTION ALGORITHM HAVING HIGHEST ENCRYPTION STRENGTH IN SET D
S1704
SELECT ENCRYPTION ALGORITHM HAVING LOWEST PROCESSING LOAD IN SET F
S1705
TO S1603
[eq. 1]:CPURecord+CPUCamera(x)≦α
CPUCamera(x):CPU RESOURCE CONSUMED BY NETWORK CAMERA APPLICATION WHEN USING ENCRYPTION ALGORITHM x

FIG. 18

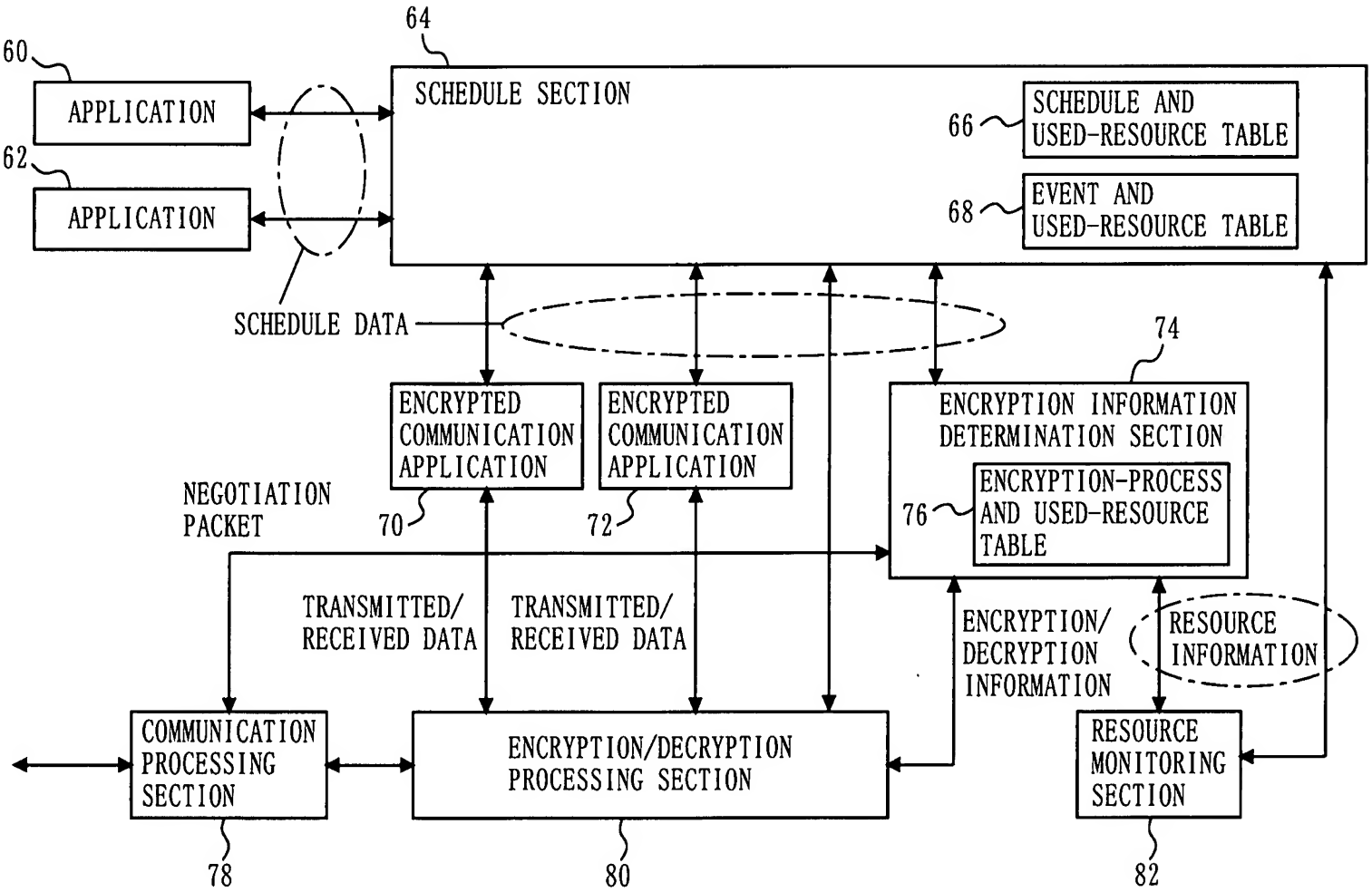
60
APPLICATION
62
APPLICATION
64
SCHEDULE SECTION
66
SCHEDULE AND USED-RESOURCE TABLE
68
EVENT AND USED-RESOURCE TABLE
SCHEDULE DATA
74
ENCRYPTED COMMUNICATION APPLICATION
ENCRYPTED COMMUNICATION APPLICATION
ENCRYPTION INFORMATION DETERMINATION SECTION
76
ENCRYPTION-PROCESS AND USED-RESOURCE TABLE
NEGOTIATION PACKET
70
72
TRANSMITTED/ RECEIVED DATA
TRANSMITTED/ RECEIVED DATA
ENCRYPTION/ DECRYPTION INFORMATION
RESOURCE INFORMATION
COMMUNICATION PROCESSING SECTION
ENCRYPTION/DECRYPTION PROCESSING SECTION
RESOURCE MONITORING SECTION
78
80
82

FIG. 19

SCHEDULE AND USED-RESOURCE TABLE IN SCHEDULE SECTION

TASK	BELONGS TO APPLICATION	START TIME	END TIME	AVERAGE USED CPU RESOURCE	AVERAGE USED MEMORY RESOURCE	AVERAGE DATA TRANSFER AMOUNT	ENCRYPTED COMMUNICATION	NECESSARY ENCRYPTION STRENGTH
TASK a	A	2002/11/1 12:00	2002/11/1 13:00	200MIPS	50MB	0Mbps	NO	—
TASK b	B	2002/11/1 14:45	— (UNKNOWN)	50MIPS	20MB	1Mbps	YES	THIRD OR HIGHER
TASK c	A	2002/11/1 12:30	2002/11/1 13:30	100MIPS	20MB	0Mbps	NO	—

("AVERAGE DATA TRANSFER AMOUNT" MEANS AVERAGE DATA TRANSFER AMOUNT FOR ENCRYPTED COMMUNICATIONS)

FIG. 20

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	AVERAGE USED MEMORY RESOURCE (MB)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	13	2
3DES-CBC	300	20	1

FIG. 21

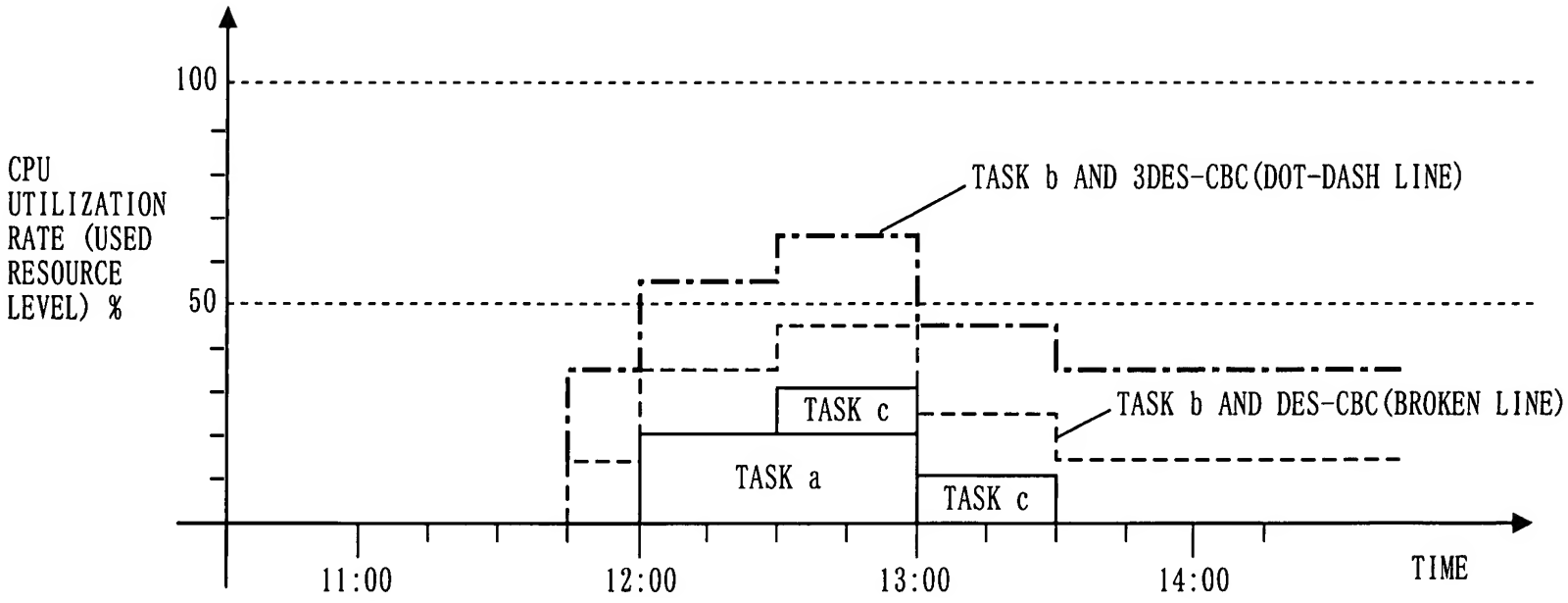
100
50
CPU UTILIZATION RATE (USED RESOURCE LEVEL) %
TASK b AND 3DES-CBC(DOT-DASH LINE)
TASK b AND DES-CBC(BROKEN LINE)
TASK c
TASK a
TASK c
11:00
12:00
13:00
14:00
TIME

FIG. 22A

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC)

EVENT TIME	TASK b		ENCRYPTION ALGORITHM		TASK a		TASK c		TOTAL USED RESOURCE
	OPERATING STATE	USED RESOURCE	ALGORITHM NAME	USED RESOURCE	OPERATING STATE	USED RESOURCE	OPERATING STATE	USED RESOURCE	
2002/11/1 11:45	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		INACTIVE		150MIPS
2002/11/1 12:00	ACTIVE	50MIPS	DES-CBC	100MIPS	ACTIVE	200MIPS	INACTIVE		350MIPS
2002/11/1 12:30	ACTIVE	50MIPS	DES-CBC	100MIPS	ACTIVE	200MIPS	ACTIVE	100MIPS	450MIPS
2002/11/1 13:00	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		ACTIVE	100MIPS	250MIPS
2002/11/1 13:30	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		INACTIVE		150MIPS

("USED RESOURCE" MEANS AVERAGE USED CPU RESOURCE)

FIG. 22B

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (3DES-CBC)

EVENT TIME	TASK b		ENCRYPTION ALGORITHM		TASK a		TASK c		TOTAL USED RESOURCE
	OPERATING STATE	USED RESOURCE	ALGORITHM NAME	USED RESOURCE	OPERATING STATE	USED RESOURCE	OPERATING STATE	USED RESOURCE	
2002/11/1 11:45	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		INACTIVE		350MIPS
2002/11/1 12:00	ACTIVE	50MIPS	3DES-CBC	300MIPS	ACTIVE	200MIPS	INACTIVE		550MIPS
2002/11/1 12:30	ACTIVE	50MIPS	3DES-CBC	300MIPS	ACTIVE	200MIPS	ACTIVE	100MIPS	650MIPS
2002/11/1 13:00	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		ACTIVE	100MIPS	450MIPS
2002/11/1 13:30	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		INACTIVE		350MIPS

("USED RESOURCE" MEANS AVERAGE USED CPU RESOURCE)

FIG. 23

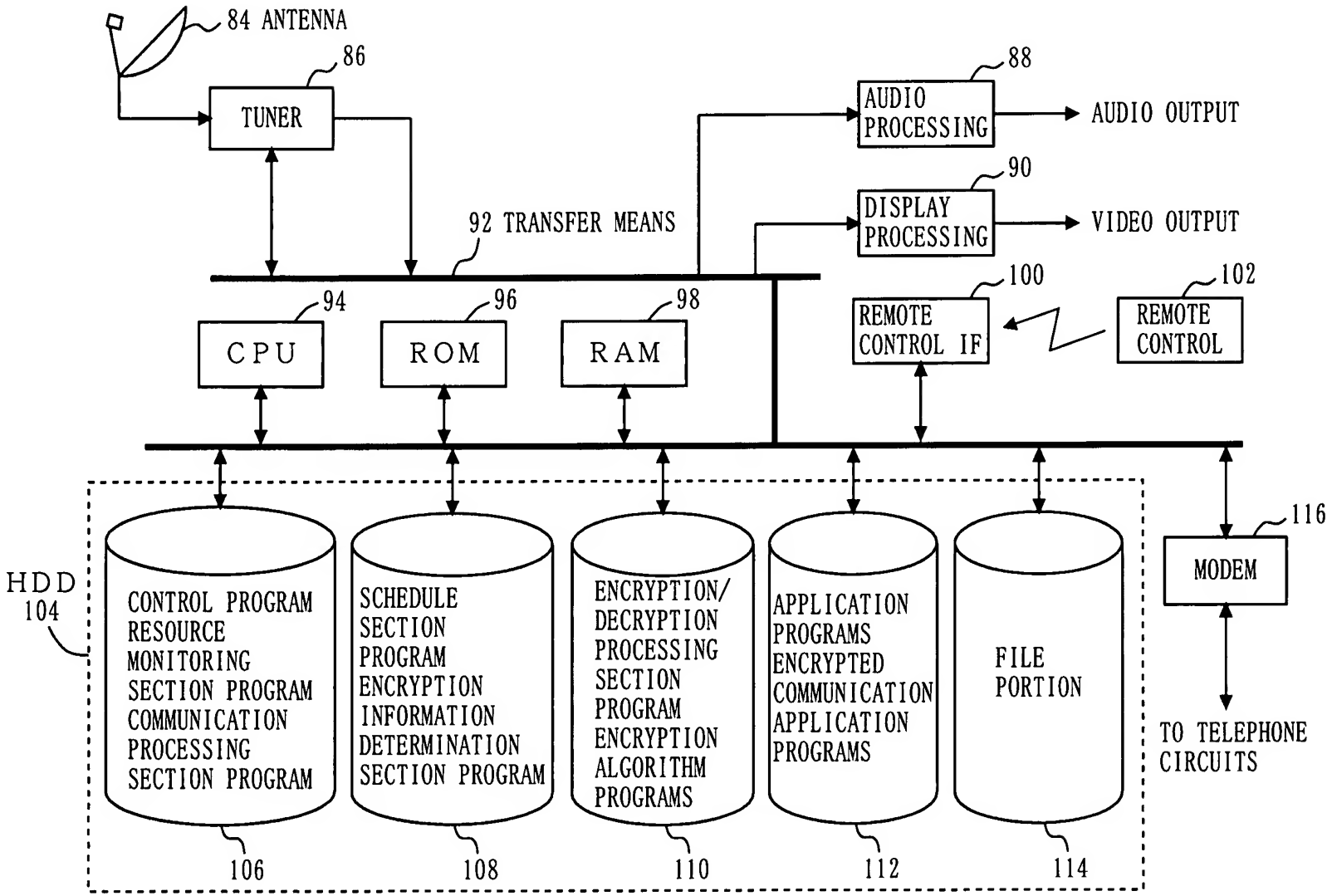
84 ANTENNA
86
TUNER
88
AUDIO PROCESSING
AUDIO OUTPUT
90
DISPLAY PROCESSING
VIDEO OUTPUT
92 TRANSFER MEANS
100
REMOTE CONTROL IF
102
REMOTE CONTROL
94
CPU
96
ROM
98
RAM
HDD 104
CONTROL PROGRAM RESOURCE MONITORING SECTION PROGRAM COMMUNICATION PROCESSING SECTION PROGRAM
SCHEDULE SECTION PROGRAM ENCRYPTION INFORMATION DETERMINATION SECTION PROGRAM
ENCRYPTION/ DECRYPTION PROCESSING SECTION PROGRAM ENCRYPTION ALGORITHM PROGRAMS
APPLICATION PROGRAMS ENCRYPTED COMMUNICATION APPLICATION PROGRAMS
FILE PORTION
106
108
110
112
114
116
MODEM
TO TELEPHONE CIRCUITS

FIG. 24

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	NUMBER OF PREPROCESS INSTRUCTIONS (MI)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	100	2
3DES-CBC	300	300	1

FIG. 25

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM
11:45	b 50			D 100	150	3D 300	350	3D
12:00	b 50	a 200		D 100	350	3D 300	550	D
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D
13:00	b 50	c 100		D 100	250	3D 300	450	3D
13:30	b 50			D 100	150	3D 300	350	3D

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 26

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	TASK/ RESOURCE	WHEN USING ALGORITHM D FOR TASK b		WHEN USING ALGORITHM 3D FOR TASK b		USED ENCRYPTION ALGORITHM
				RESOURCE	TOTAL RESOURCE	RESOURCE	TOTAL RESOURCE	
11:45	b 50			100	150	300	350	3D
12:00	b 50	a 200		100	350	300	550	D
12:30	b 50	a 200	c 100	100	450	300	650	D
13:00	b 50	C 100		100	250	300	450	3D
13:30	b 50			100	150	300	350	3D

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 27

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM	PREPROCESS	PREPROCESS ENCRYPTION ALGORITHM
11:42									Mt1	3D
11:45	b 50			D 100	150	3D 300	350	3D		
11:58	SAME AS ABOVE			SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	3D	Mt2	D
12:00	b 50	a 200		D 100	350	3D 300	550	D		
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D		
12:56	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	D	Mt3	3D
13:00	b 50	c 100		D 100	250	3D 300	450	3D		
13:30	b 50			D 100	150	3D 300	350	3D		

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 28

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC, AES)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM	PREPROCESS	PREPROCESS ENCRYPTION ALGORITHM
11:43											Mt1	A
11:45	b 50			D 100	150	3D 300	350	A 200	250	A		
12:00	b 50	a 200		D 100	350	3D 300	550	A 200	450	A		D
12:29	SAME AS ABOVE	SAME AS ABOVE		SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	A	Mt2	
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	A 200	550	D		
12:58	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	D	Mt3	A
13:00	b 50	c 100		D 100	250	3D 300	450	A 200	350	A		
13:30	b 50			D 100	150	3D 300	350	A 200	250	A		

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC; "A" MEANS AES)

FIG. 29

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	AVERAGE USED MEMORY RESOURCE (MB)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	13	3
3DES-CBC	300	20	2
AES	200	16	1

FIG. 30

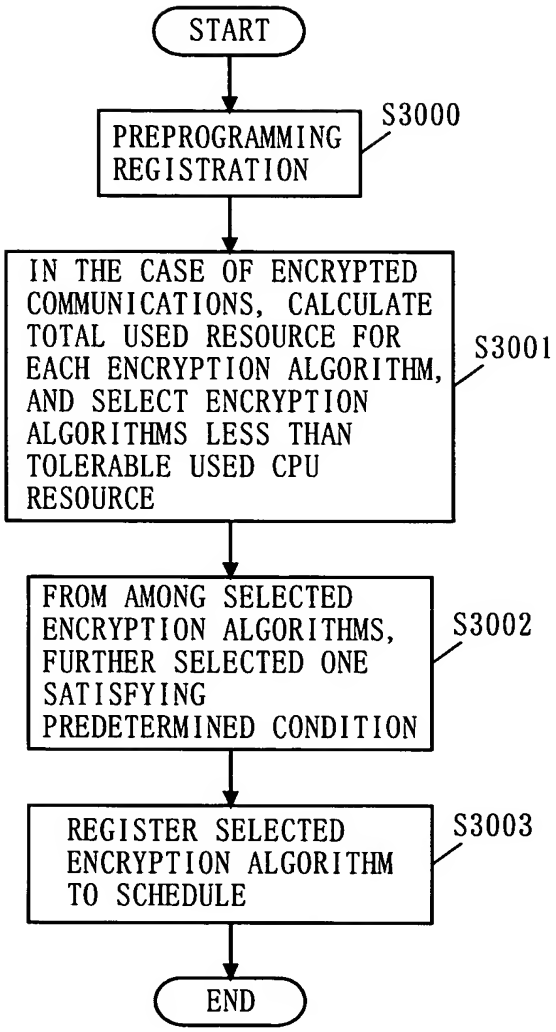
START
PREPROGRAMMING REGISTRATION
S3000
IN THE CASE OF ENCRYPTED COMMUNICATIONS, CALCULATE TOTAL USED RESOURCE FOR EACH ENCRYPTION ALGORITHM, AND SELECT ENCRYPTION ALGORITHMS LESS THAN TOLERABLE USED CPU RESOURCE
S3001
FROM AMONG SELECTED ENCRYPTION ALGORITHMS, FURTHER SELECTED ONE SATISFYING PREDETERMINED CONDITION
S3002
REGISTER SELECTED ENCRYPTION ALGORITHM TO SCHEDULE
S3003
END

FIG. 31

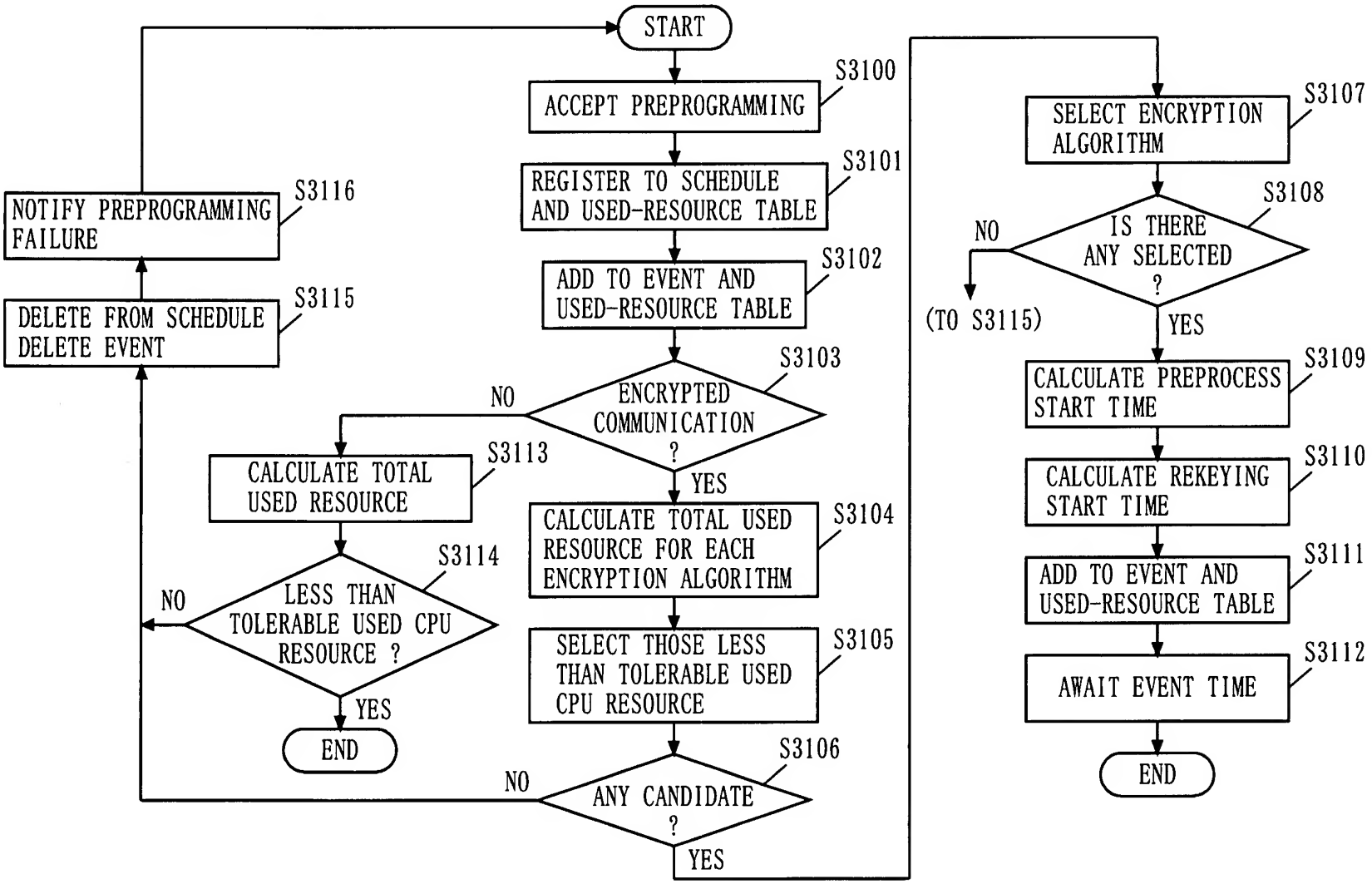
START
ACCEPT PREPROGRAMMING
S3100
REGISTER TO SCHEDULE AND USED-RESOURCE TABLE
S3101
ADD TO EVENT AND USED-RESOURCE TABLE
S3102
ENCRYPTED COMMUNICATION ?
S3103
NO
YES
CALCULATE TOTAL USED RESOURCE FOR EACH ENCRYPTION ALGORITHM
S3104
SELECT THOSE LESS THAN TOLERABLE USED CPU RESOURCE
S3105
ANY CANDIDATE ?
S3106
NO
YES
SELECT ENCRYPTION ALGORITHM
S3107
IS THERE ANY SELECTED ?
S3108
NO
(TO S3115)
YES
CALCULATE PREPROCESS START TIME
S3109
CALCULATE REKEYING START TIME
S3110
ADD TO EVENT AND USED-RESOURCE TABLE
S3111
AWAIT EVENT TIME
S3112
END
CALCULATE TOTAL USED RESOURCE
S3113
LESS THAN TOLERABLE USED CPU RESOURCE ?
S3114
NO
YES
END
DELETE FROM SCHEDULE DELETE EVENT
S3115
NOTIFY PREPROGRAMMING FAILURE
S3116

FIG. 32

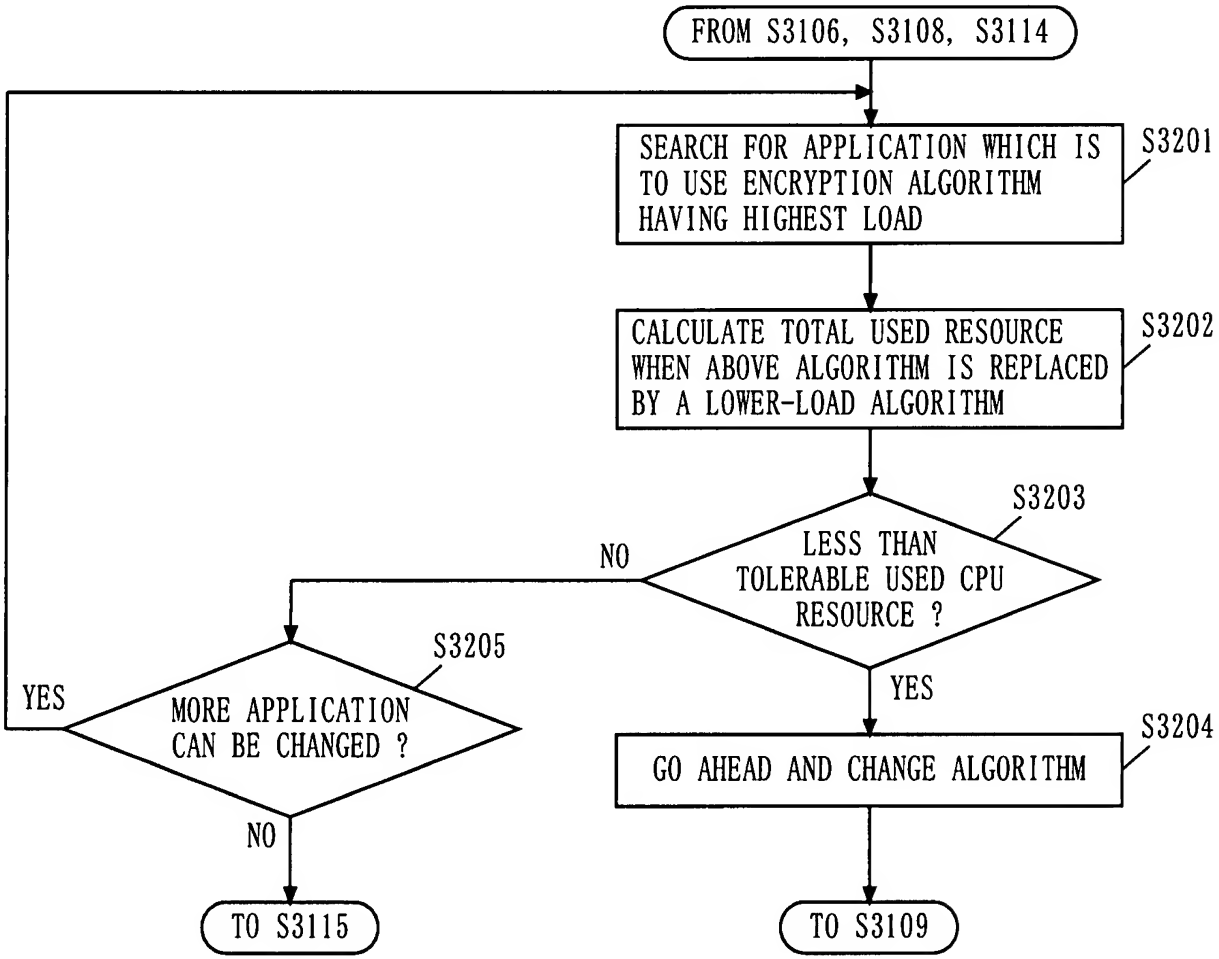
FROM S3106, S3108, S3114
SEARCH FOR APPLICATION WHICH IS TO USE ENCRYPTION ALGORITHM HAVING HIGHEST LOAD
S3201
CALCULATE TOTAL USED RESOURCE WHEN ABOVE ALGORITHM IS REPLACED BY A LOWER-LOAD ALGORITHM
S3202
S3203
LESS THAN TOLERABLE USED CPU RESOURCE ?
NO
YES
S3205
MORE APPLICATION CAN BE CHANGED ?
YES
NO
S3204
GO AHEAD AND CHANGE ALGORITHM
TO S3115
TO S3109

FIG. 33

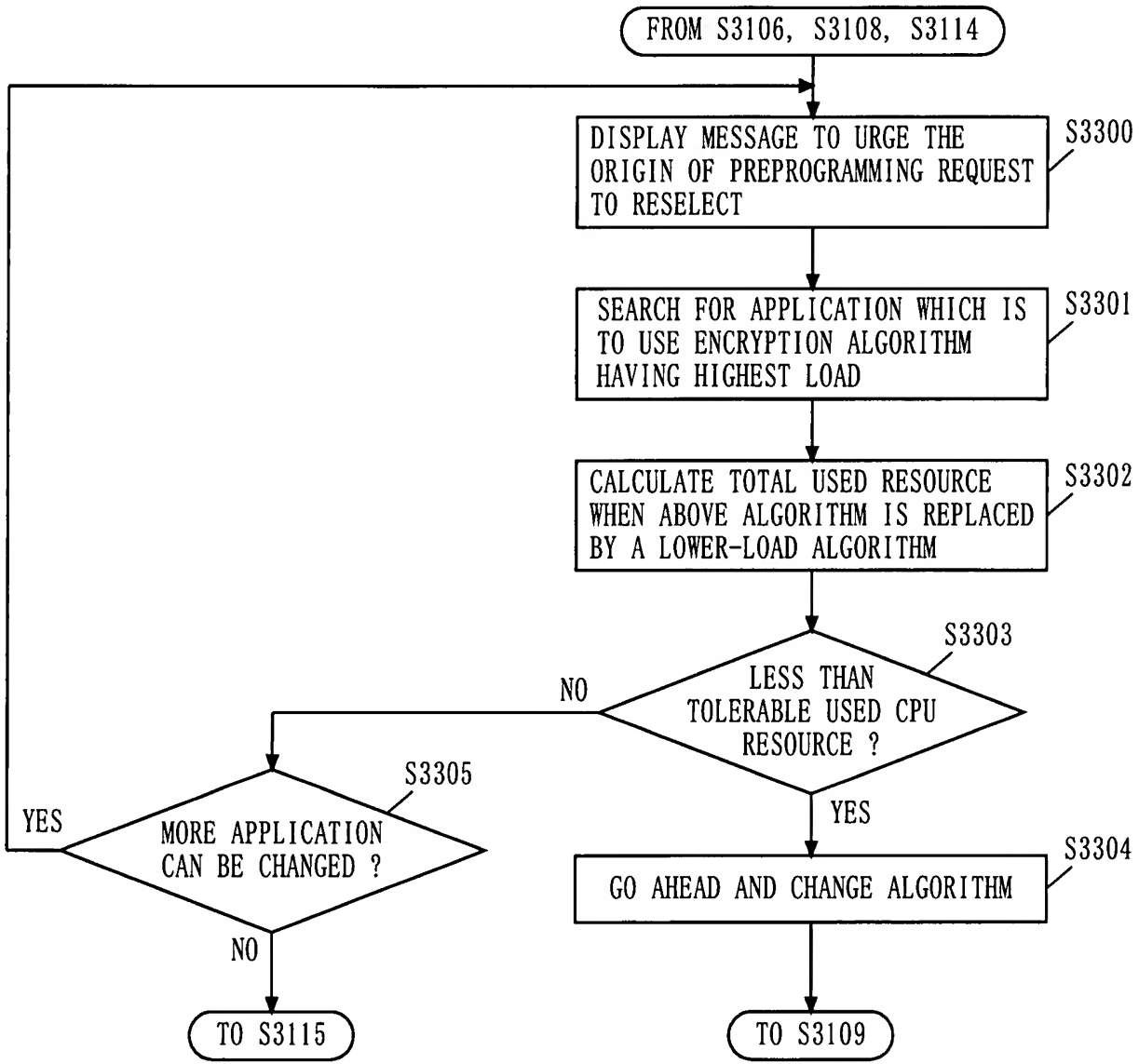
FROM S3106, S3108, S3114
DISPLAY MESSAGE TO URGE THE ORIGIN OF PREPROGRAMMING REQUEST TO RESELECT
S3300
SEARCH FOR APPLICATION WHICH IS TO USE ENCRYPTION ALGORITHM HAVING HIGHEST LOAD
S3301
CALCULATE TOTAL USED RESOURCE WHEN ABOVE ALGORITHM IS REPLACED BY A LOWER-LOAD ALGORITHM
S3302
S3303
LESS THAN TOLERABLE USED CPU RESOURCE ?
NO
YES
S3305
MORE APPLICATION CAN BE CHANGED ?
YES
NO
S3304
GO AHEAD AND CHANGE ALGORITHM
TO S3115
TO S3109

FIG. 34

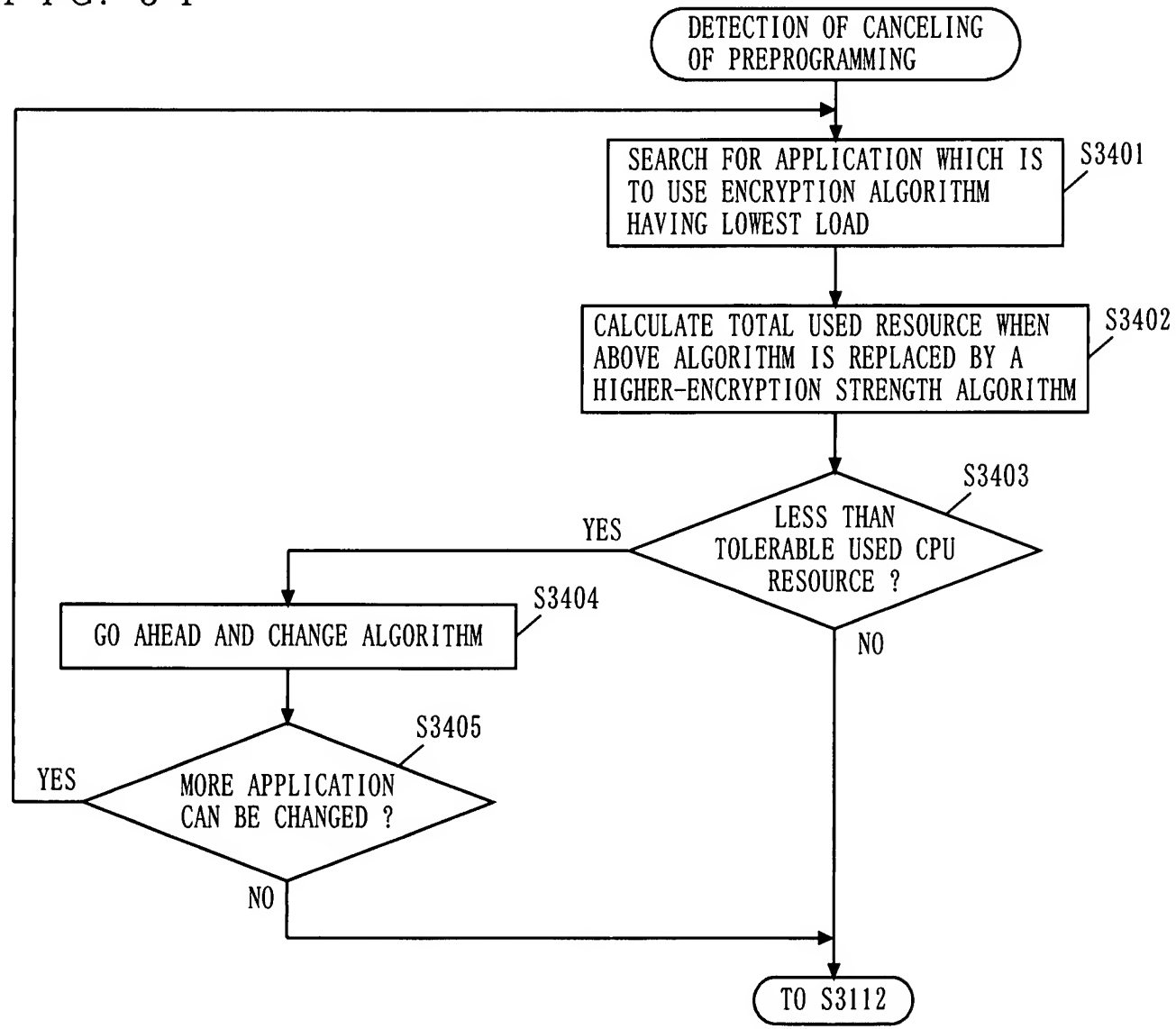
DETECTION OF CANCELING OF PREPROGRAMMING
SEARCH FOR APPLICATION WHICH IS TO USE ENCRYPTION ALGORITHM HAVING LOWEST LOAD
S3401
CALCULATE TOTAL USED RESOURCE WHEN ABOVE ALGORITHM IS REPLACED BY A HIGHER-ENCRYPTION STRENGTH ALGORITHM
S3402
S3403
LESS THAN TOLERABLE USED CPU RESOURCE ?
YES
NO
GO AHEAD AND CHANGE ALGORITHM
S3404
S3405
MORE APPLICATION CAN BE CHANGED ?
YES
NO
TO S3112

FIG. 35

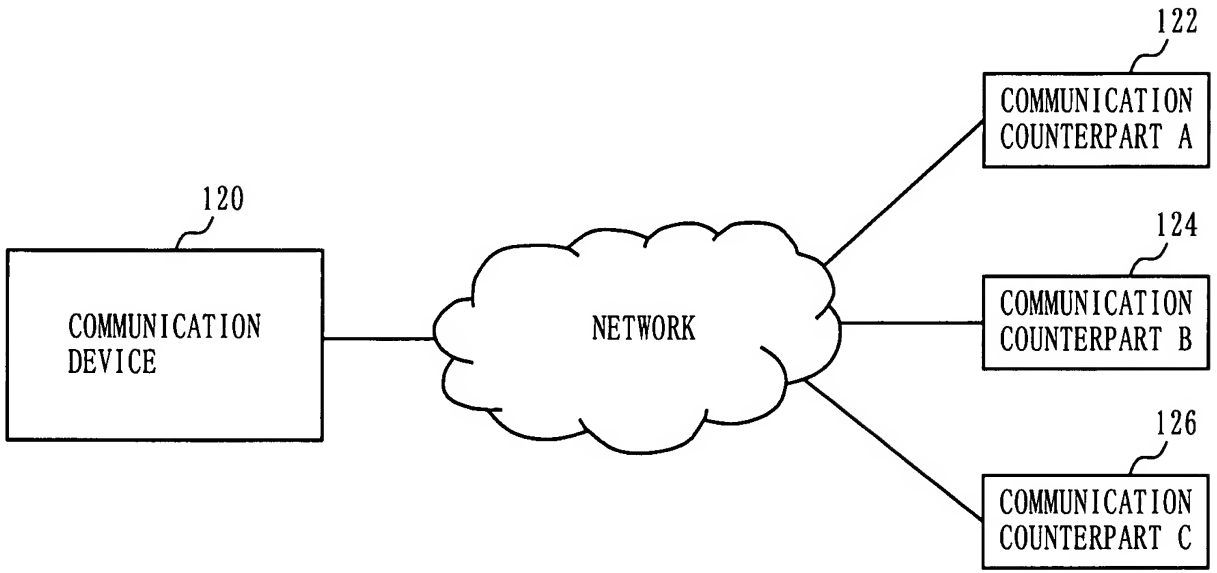
120
COMMUNICATION DEVICE
NETWORK
122
COMMUNICATION COUNTERPART A
124
COMMUNICATION COUNTERPART B
126
COMMUNICATION COUNTERPART C

FIG. 36

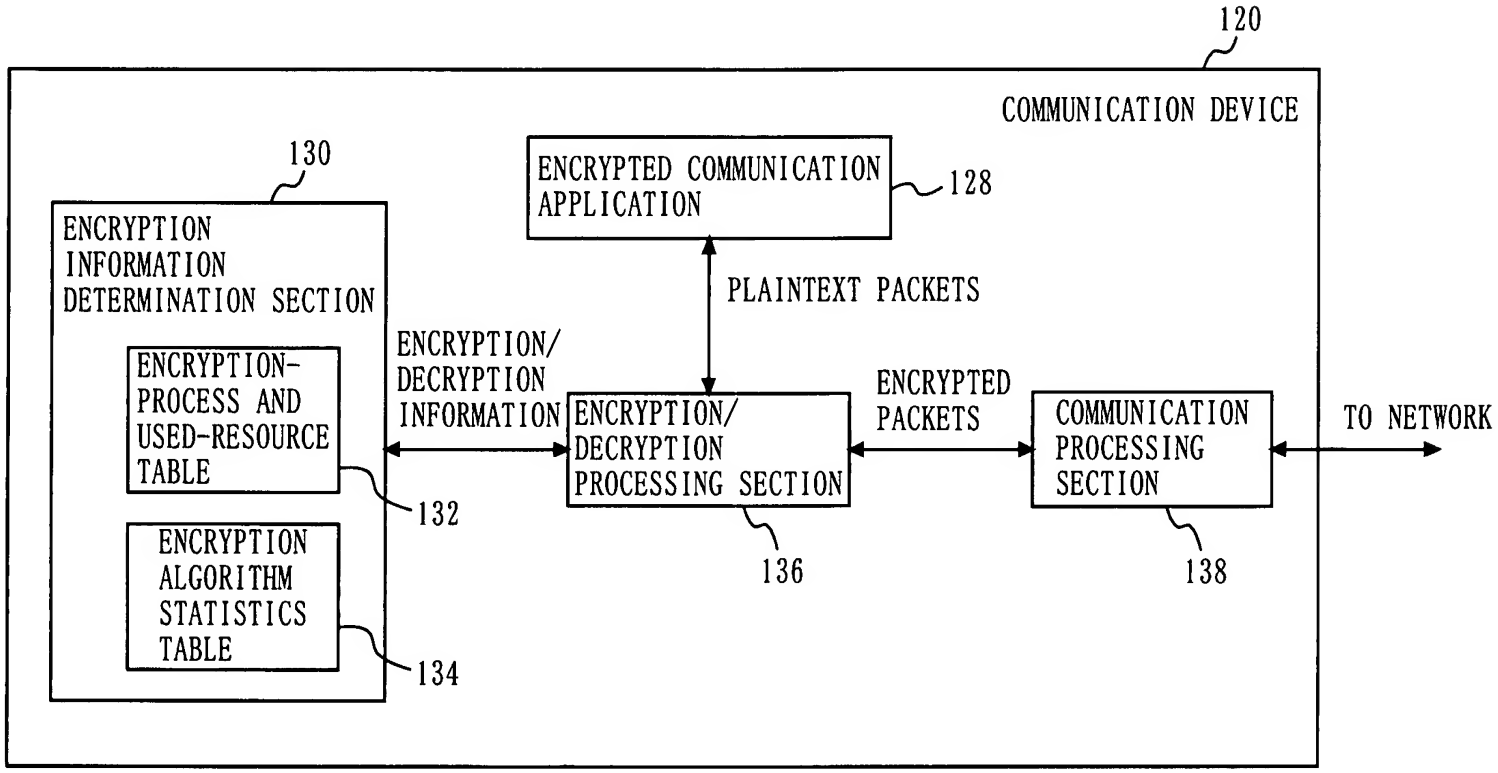
120
COMMUNICATION DEVICE
130
ENCRYPTION INFORMATION DETERMINATION SECTION
ENCRYPTION-PROCESS AND USED-RESOURCE TABLE
132
ENCRYPTION ALGORITHM STATISTICS TABLE
134
ENCRYPTED COMMUNICATION APPLICATION
128
PLAINTEXT PACKETS
ENCRYPTION/ DECRYPTION INFORMATION
ENCRYPTION/ DECRYPTION PROCESSING SECTION
136
ENCRYPTED PACKETS
COMMUNICATION PROCESSING SECTION
138
TO NETWORK

FIG. 37

ALGORITHM	CALCULATION AMOUNT	CALCULATION AMOUNT INDEX (ORDER)	ENCRYPTION STRENGTH (ORDER)
DES-CBC	100	1	3
3DES-CBC	300	3	2
AES-CBC	200	2	1

FIG. 38

COMMUNICATION COUNTERPART	last	FREQUENCY		
		DES	3DES	AES
COMMUNICATION COUNTERPART A	3DES-CBC	17	3	*
COMMUNICATION COUNTERPART B	3DES-CBC	*	13	7
COMMUNICATION COUNTERPART C	AES-CBC	*	5	15

FIG. 39

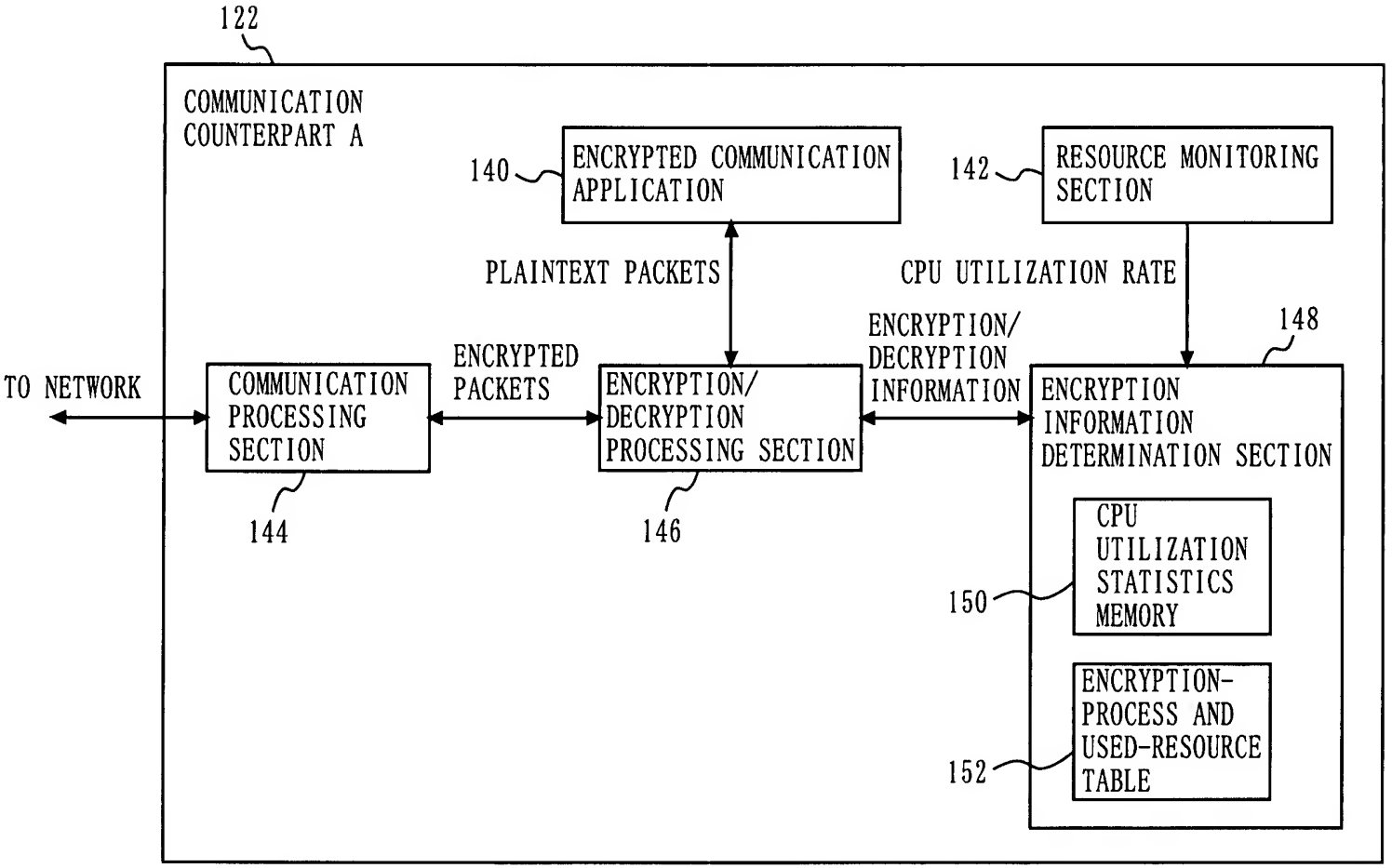
122
COMMUNICATION COUNTERPART A
140
ENCRYPTED COMMUNICATION APPLICATION
142
RESOURCE MONITORING SECTION
PLAINTEXT PACKETS
CPU UTILIZATION RATE
ENCRYPTION/ DECRYPTION INFORMATION
148
TO NETWORK
COMMUNICATION PROCESSING SECTION
ENCRYPTED PACKETS
ENCRYPTION/ DECRYPTION PROCESSING SECTION
ENCRYPTION INFORMATION DETERMINATION SECTION
144
146
CPU UTILIZATION STATISTICS MEMORY
150
ENCRYPTION-PROCESS AND USED-RESOURCE TABLE
152

FIG. 40

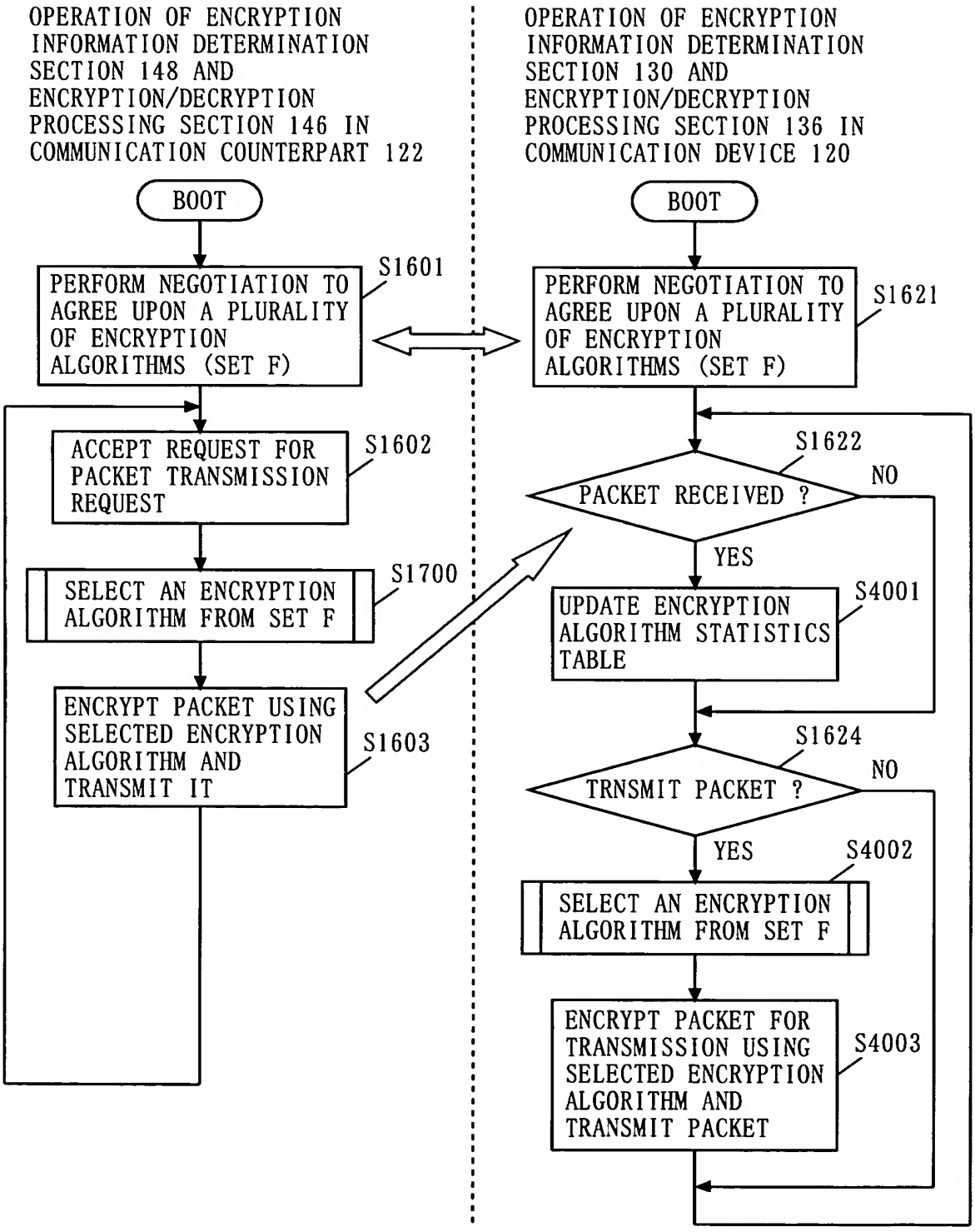
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 148 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 146 IN COMMUNICATION COUNTERPART 122
OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 130 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 136 IN COMMUNICATION DEVICE 120
BOOT
BOOT
PERFORM NEGOTIATION TO AGREE UPON A PLURALITY OF ENCRYPTION ALGORITHMS (SET F)
S1601
PERFORM NEGOTIATION TO AGREE UPON A PLURALITY OF ENCRYPTION ALGORITHMS (SET F)
S1621
ACCEPT REQUEST FOR PACKET TRANSMISSION REQUEST
S1602
S1622
PACKET RECEIVED ?
NO
YES
SELECT AN ENCRYPTION ALGORITHM FROM SET F
S1700
UPDATE ENCRYPTION ALGORITHM STATISTICS TABLE
S4001
ENCRYPT PACKET USING SELECTED ENCRYPTION ALGORITHM AND TRANSMIT IT
S1603
S1624
TRNSMIT PACKET ?
NO
YES
S4002
SELECT AN ENCRYPTION ALGORITHM FROM SET F
ENCRYPT PACKET FOR TRANSMISSION USING SELECTED ENCRYPTION ALGORITHM AND TRANSMIT PACKET
S4003

FIG. 41

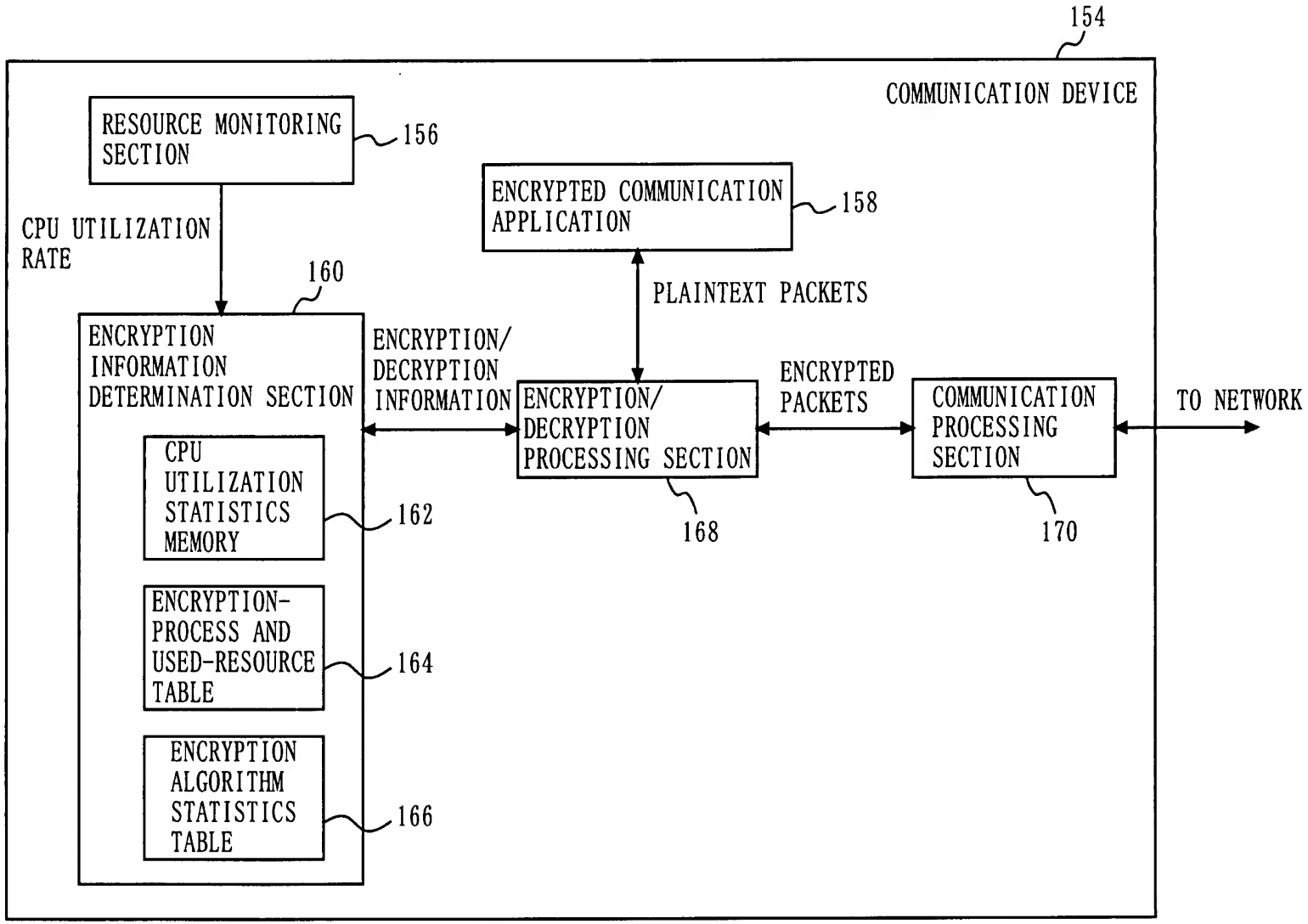
154
COMMUNICATION DEVICE
RESOURCE MONITORING SECTION
156
CPU UTILIZATION RATE
ENCRYPTED COMMUNICATION APPLICATION
158
PLAINTEXT PACKETS
160
ENCRYPTION INFORMATION DETERMINATION SECTION
ENCRYPTION/ DECRYPTION INFORMATION
ENCRYPTION/ DECRYPTION PROCESSING SECTION
ENCRYPTED PACKETS
COMMUNICATION PROCESSING SECTION
TO NETWORK
CPU UTILIZATION STATISTICS MEMORY
162
168
170
ENCRYPTION-PROCESS AND USED-RESOURCE TABLE
164
ENCRYPTION ALGORITHM STATISTICS TABLE
166

FIG. 42 PRIOR ART

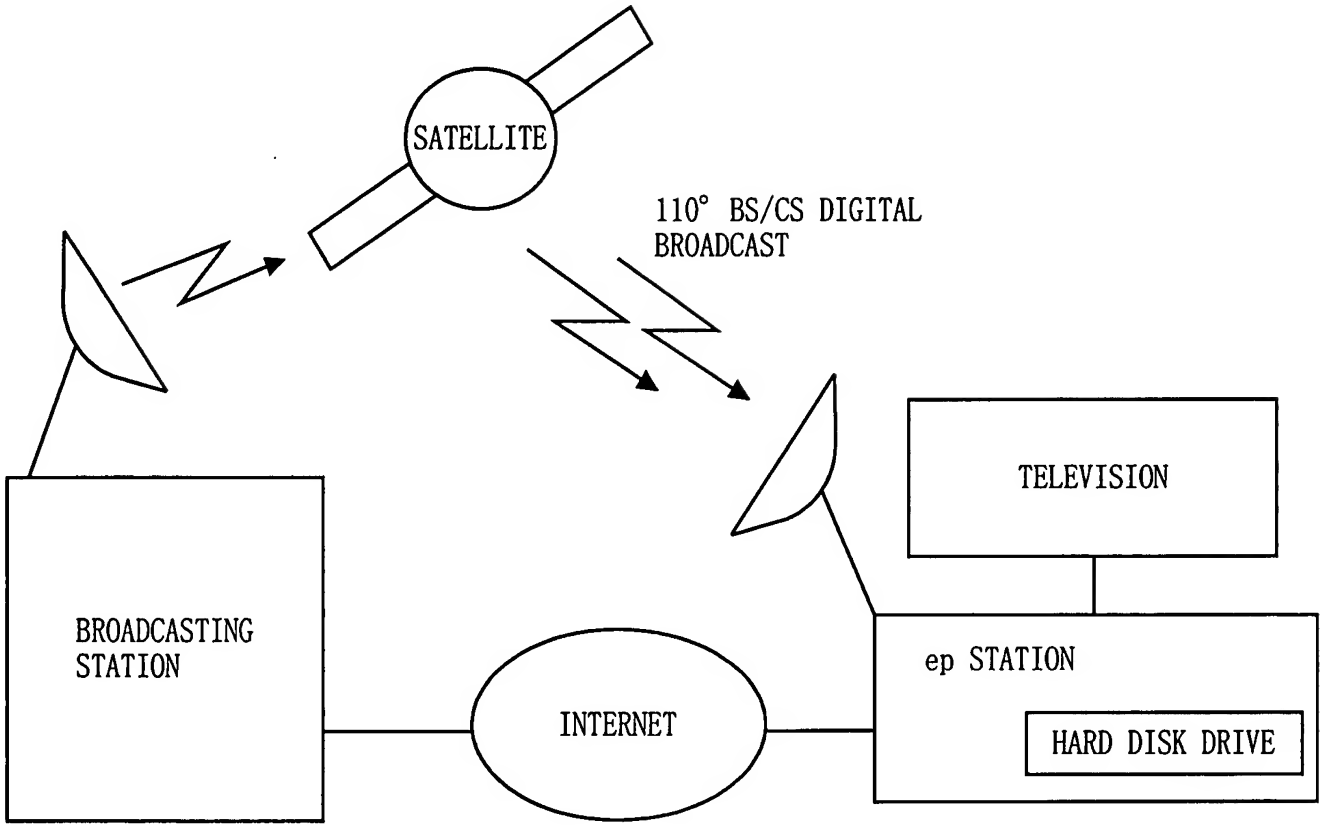

FIG. 43 PRIOR ART

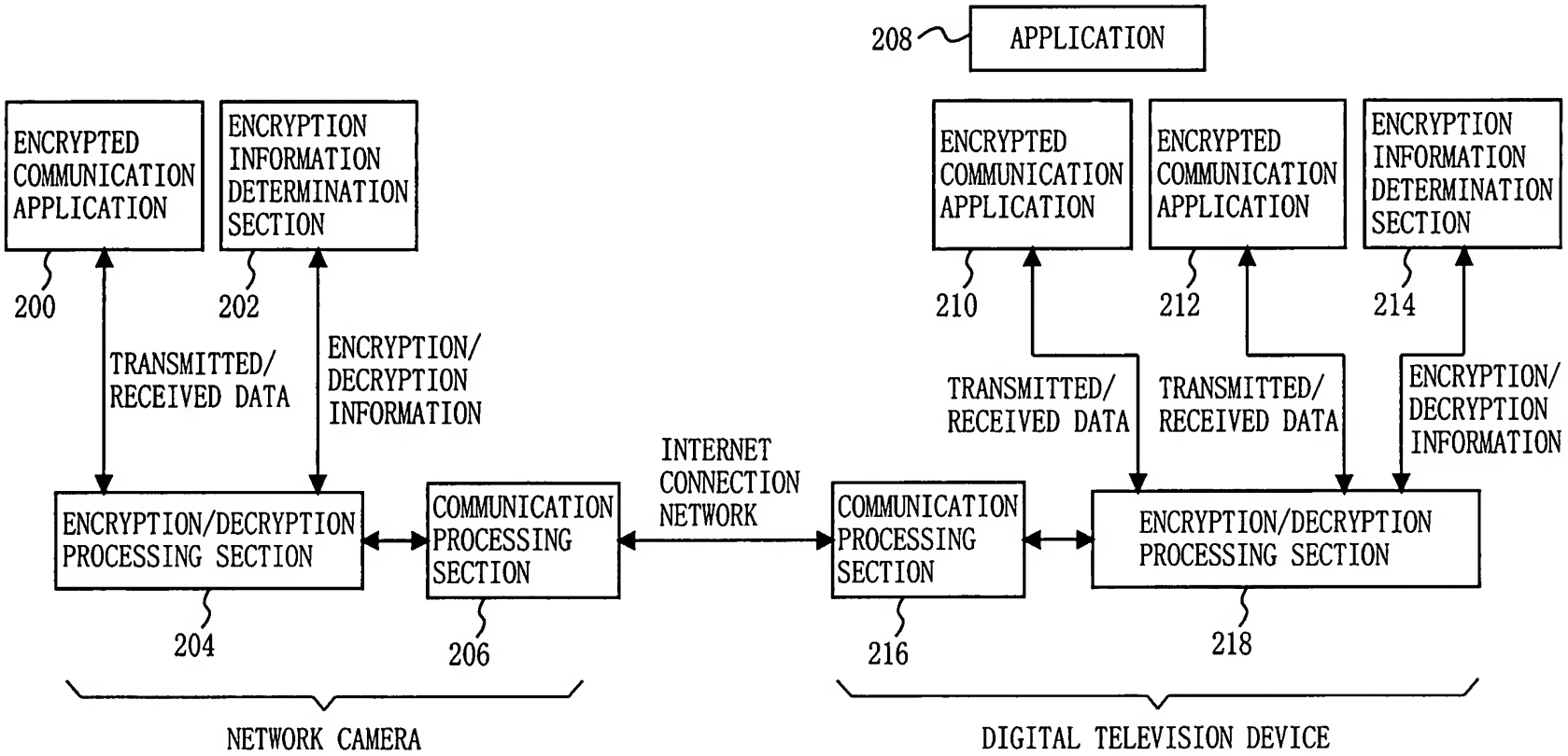
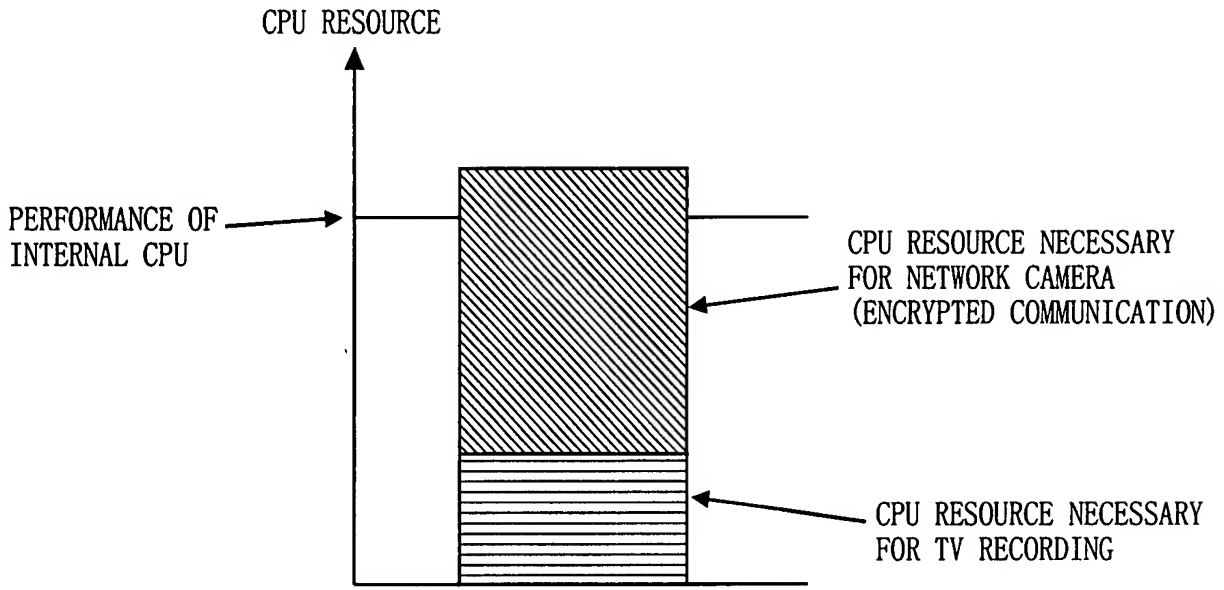
FIG. 44 PRIOR ART